IPBrick
Manuel de Référence
Version 4.0

iPortalMais - Serviços de Internet e Redes, Lda.

Août 2006

Copyright ©iPortalMais
Tous les droits réservés. Septembre 2002. L'information contenue dans ce document est soumise à changements sans avis préalable. Les déclarations, les donnés techniques, les configuretions et les recommandations de ce document sont prétendument précises et fiables, mais elles sont présentées sans garanties expresses ou implicites.

Table des matières

1 Objet de ce document **11**

2 Avant de commencer **13**

3 *IPBrick.I* **15**
3.1 Gestion de Machines . . . 15
3.2 Groupes . . . 18
3.3 Gestion des Utilisateurs . . . 23
3.4 Serveur de Domaine . . . 28
3.5 Las aires de Travaux . . . 28
3.5.1 Individuels . . . 28
3.5.2 Groupe . . . 32
3.5.3 Kaspersky . . . 36
3.6 Courrier Électronique . . . 36
3.6.1 Configurer . . . 36
3.6.2 Gestion de Files d'attente . . . 41
3.6.3 Adresses Alternatives . . . 42
3.6.4 Guider le Courrier . . . 44
3.6.5 Réponses Automatiques . . . 44
3.6.6 Kaspersky Anti-Vírus . . . 46
3.7 Serveur Imprimante . . . 47
3.8 Serveur Sauvegarde . . . 49

4 *IPBrick.C* **51**
4.1 Firewall . . . 51
4.1.1 Services Disponibles . . . 51
4.1.2 Bloquer les Services . . . 52
4.2 Proxy . . . 54
4.2.1 Configuration . . . 54
4.2.2 Statistiques . . . 56
4.2.3 Kaspersky Proxy . . . 56
4.3 VPN . . . 56
4.3.1 PPTP . . . 59
4.3.2 IPSec . . . 60
4.3.3 SSL . . . 62
4.4 Courrier Électronique . . . 63
4.4.1 Chercher courrier dans l'ISP . . . 65

4.4.2 Copie du courrier . . . 68
4.4.3 Kaspersky Anti-Vírus . . . 69
4.4.4 Kaspersky Anti-Spam . . . 69
4.5 Serveur Web . . . 69
4.6 Webmail . . . 76
4.6.1 Serveurs . . . 76
4.7 VoIP . . . 76
4.7.1 Téléphones Enregistrés . . . 78
4.7.2 Adresses Alternatives . . . 80
4.7.3 Téléphones Actives . . . 80
4.7.4 Bloquage d' Appels . . . 80
4.7.5 Statistiques des Appels . . . 82
4.7.6 Gestion des Routes . . . 83
4.7.7 Séq. de réponse . . . 84

5 Définitions Avancées 85
5.1 *IPBrick* . . . 85
5.1.1 Définitions . . . 85
5.1.2 Informations du système . . . 86
5.1.3 Accès . . . 86
5.1.4 Authentification . . . 90
5.1.5 Multitraitement . . . 93
5.2 Téléphonie . . . 94
5.3 Réseau . . . 95
5.3.1 Pare-feu . . . 96
5.3.2 Gestion de Routes . . . 98
5.3.3 QoS . . . 99
5.4 Services d'appu . . . 101
5.4.1 Gestion de machines . . . 101
5.4.2 DNS . . . 101
5.4.3 DHCP . . . 109
5.4.4 Serveur de Machines . . . 114
5.5 Configuration . . . 115
5.5.1 Restituer . . . 115
5.5.2 Télécharger . . . 115
5.5.3 Upload . . . 115
5.6 Système . . . 119
5.6.1 Services . . . 119
5.6.2 Gestion de tâches . . . 120
5.6.3 Date et l'heure . . . 120
5.6.4 Logs du Système . . . 120
5.6.5 SSH . . . 123
5.6.6 Recommencer . . . 123
5.6.7 Débrancher . . . 124

6 Actualiser les Définitions 127

7 Annexe A - Placement du domaine 129
7.1 Placement d'une machine dans un domaine 129
7.1.1 Postes de travaille Windows XP Professionnel 129

8 Annexe B - Placement d'une connexion VPN 133
8.1 Placement d'une connexion VPN (PPTP) 133

9 Annexe C - Configuration d' une liaison VPN SSL (OpenVPN) 135
9.1 Configuration d' une liaison VPN SSL (OpenVPN) 135
9.1.1 Deux ou plus certificats SSL 135

Table des figures

3.1 Gestion de Machines 16
3.2 Gestion de Machines - Insérer 17
3.3 Gestion de Machines - Changer 18
3.4 Gestion de Machines - Effacer 19
3.5 Groupes - Insérer 20
3.6 Groupes - Listage 21
3.7 Groupes - Définition des Utilisateurs 22
3.8 Gestion des Utilisateurs - Liste 24
3.9 Gestion des Utilisateurs - Insérer 25
3.10 Gestion des Utilisateurs - Détail 26
3.11 Gestion des Utilisateurs - Changer 27
3.12 Serveur de Domaine 29
3.13 Aires de travail - Résumé 30
3.14 Aires de Travail - Résumé des Aires Individuelles 31
3.15 Aires de Travail - Individuels 32
3.16 Secteurs de Travail - Groupe - Insertion 33
3.17 Secteurs de Travail - Groupe - Gestion 34
3.18 Secteurs de Travail - Groupe - Accès Groupes 35
3.19 Secteurs de Travail - Kaspersky 37
3.20 Courrier Électronique - Configurer 39
3.21 Courrier Électronique - Gestion de files d'attente 41
3.22 Courrier Électronique - Adresses Alternatives 43
3.23 Guider le Courrier 44
3.24 Guider le Courrier - Insertion des comptes 45
3.25 Courrier Électronique - Réponses Automatiques 46
3.26 Insérer une imprimante de réseau 48
3.27 Insérer une imprimante en réseau 49
3.28 Serveur Sauvegarde 50

4.1 Pare-feu - Services Disponibles 52
4.2 Pare-feu - Bloquer les Services 53
4.3 Proxy - Configuretion 54
4.4 Proxy - Statistiques de Cache 57
4.5 Proxy - Statistiques par l'utilisateur 58
4.6 VPN - Utilisateurs 59
4.7 VPN - IPSec 61
4.8 VPN - SSL 62

4.9 Chercher Courrier dans l'ISP - Insérer ISP 64
4.10 Chercher Courrier dans l'ISP - Gestion des Serveurs 65
4.11 Chercher Courrier dans l'ISP - Gestion de comptes 66
4.12 Chercher courrier dans l'ISP - insertion des comptes 67
4.13 Copie du courrier 68
4.14 Kaspersky Anti-Vírus 70
4.15 Kaspersky Anti-Spam 71
4.16 Serveur Web - Liste des Sites 72
4.17 Serveur Web - Insertion de Sites 73
4.18 Serveur Web - Gestion du Site 74
4.19 Serveur Web - Gestion de Alias 75
4.20 WebMail - serveurs 77
4.21 Téléphones Enregistrés 78
4.22 VoIP - Options 79
4.23 Adresses Alternatives 80
4.24 Téléphones Actives 81
4.25 VoIP - Bloquage d' Appels 82
4.26 VoIP - Gestion des Routes 83

5.1 Définitions de l'*IPBrick* 87
5.2 Informations du système 88
5.3 Login d'accès 89
5.4 Idiome 90
5.5 Authentification 91
5.6 Multitraitement 93
5.7 Téléphonie - Insérer 94
5.8 Téléphonie 95
5.9 Réseau - Pare-feu 96
5.10 Réseau - Gestion de Routes 98
5.11 Réseau - QoS 99
5.12 Réseau - Gestion QoS 100
5.13 DNS - Domaines 102
5.14 DNS - Insérer Zones de résolution directe et inverse 103
5.15 DNS - Gestion de domaines 105
5.16 DNS - Forwarders 107
5.17 DNS - Résolution des Noms 108
5.18 DHCP - Sub-réseau 109
5.19 DHCP - Définitions Avancées 110
5.20 DHCP - Définitions Sub-réseau 111
5.21 Redondance 113
5.22 DHCP - Machines 114
5.23 Restituer Configuration 116
5.24 Décharger Configuration 117
5.25 Charger Configuration éloignées 118
5.26 Services 119
5.27 Date et l'heure du système 121

5.28 Logs du Système 122
5.29 SSH 123
5.30 Recommencer le Serveur 124
5.31 Débrancher le serveur 125

6.1 Actualiser les Définitions 127

Chapitre 1

Objet de ce document

Ce manuel contient information sur les menus de l'*IPBrick*. Il a une description détaillée sur :

- Configuretion de l'*IPBrick.I* ;
- Configuretion de l'*IPBrick.C* ;
- Configuretion avancées.

Les autres chapitres de ce manuel sont sur les configuretions des postes de travail. Les configuretions décrites sont :

- Conduite pour le placement d'une poste de travail (MS Windows) dans un domaine ;
- Conduite pour l'établissement d'un réseau privé virtuel (VPN) PPTP et SSL.

Chapitre 2

Avant de commencer

Au établir la session WEB avec l'*IPBrick* est présentée dans une page Web pour une légalisation. Après la validation correcte, la première page Web de contact avec l'*IPBrick* vous permet de changer le domaine et les réseaux IP des interfaces privées et publiques du serveur.

! Attention: Si le réseau de communications où vous installez une *IPBrick* a déjà un serveur de DHCP et de Domaine, ces deux fonctionnalités devront être désactivées afin d'éviter des conflits.

Pour obtenir autres informations sur la façon d'installer l'*IPBrick* et configurer la poste de travail pour accéder à *IPBrick*, consultez le manuel d'installation. L'interface Web de gestion de l'*IPBrick* est partagée en 3 menus principaux :

- *IPBrick.I* ;
- *IPBrick.C* ;
- Définitions Avancées ;
- Actualiser les Définitions ;

Dans l'*IPBrick.I* on configure les services basiques d'une Intranet et dans l'*IPBrick.C* on configure les services basiques de communications. Le menu `Définitions Avancées` permet faire `Configuretions supplémentaires` aux services basiques et obtenir des informations sur l'état de fonctionnement de l'*IPBrick*. Quelque configuretion faite dans l'*IPBrick* devient accomplie après un `Actualiser Définitions`. Les changements dans la configuretion des menus :

- `Définitions Avancées` » *IPBrick* » `Définitions` ;
- `Définitions Avancées` » *IPBrick* » `Légalisation` ;
- `Définitions Avancées` » *IPBrick* » `Multiprocesseur` ;

ils obligent l'*IPBrick* à recommencer (l'*IPBrick* a besoin d'un minute pour recommencer, ça dépend de l'hardware où elle est installée).

Il faut placer une PenDrive dans le serveur où l'*IPBrick* est installée, elle garde les configuretions actuelles du système quand l'administrateur fait `Actualiser Définitions`. De cette façon, on a la chance d'avoir une plus de valeurs de l'*IPBrick*, le Disaster Recovery, comme par exemple, en cas de panne du disque, il est possible par l'configuretions existantes. Dans l'interface de gestion, il y a plusieurs liens qui permettent surfer dans l'*IPBrick*.

Ces liens sont :

- `Tourner` : permet tourner à la page antérieur sans garder éventuelles altérations

faites ;
- `Insérer` : permet insérer nouveaux items ;
- `Changer` : permet changer les définitions d'un itemm ;
- `Effacer` : permet éliminer un item.

Chapitre 3

IPBrick.I

Ce chapitre décrit les menus de l'*IPBrick* utilisés pour commander les principaux services d'une Intranet. Le chapitre a les suivantes sections principales :

- Gestion de machines ;
- Groupes ;
- Gestion d'utilisateurs ;
- Serveur de domaine ;
- Secteurs de travail ;
- Courrier Électronique ;
- Serveur Imprimante ;
- Serveur de backup.

3.1 Gestion de Machines

Cette section permet ajouter et changer le registre de machines (e.g., PC, portable, imprimante).

Une machine est présentée par le nom, un adresse IP, un adresse MAC et dela façon, comme il est présenté dans la Fig. 3.1. Ils sont considérés trois types de machines :

- WorkStation ;
- IP Phone ;
- WorkStation + SoftPhone ;

Pour insérer une machine est seulement nécessaire définir le type, introduire le nom et un adresse IP (Fig. 3.2). De cette façon, le registre de la machine sera créé dans le LDAP et dans le serveur DNS. Si le champ Adresse MAC sera rempli avec l'adresse MAC de la machine a registrer, sera aussi crée une rentrée dans le serveur DHCP pou cette machine.

⇒ **Remarque: L'adresse MAC d'une machine peut être obtenu dans le Windows XP dans l'icône de Connexion de réseau, ou dans la ligne des commandes en exécutant le command ipconfig /all.**

- Le nom de l'ordinateur doit être constitué par des caractères exclusivement alphanúmeriques. La seule exception est les caractères _ et - ;

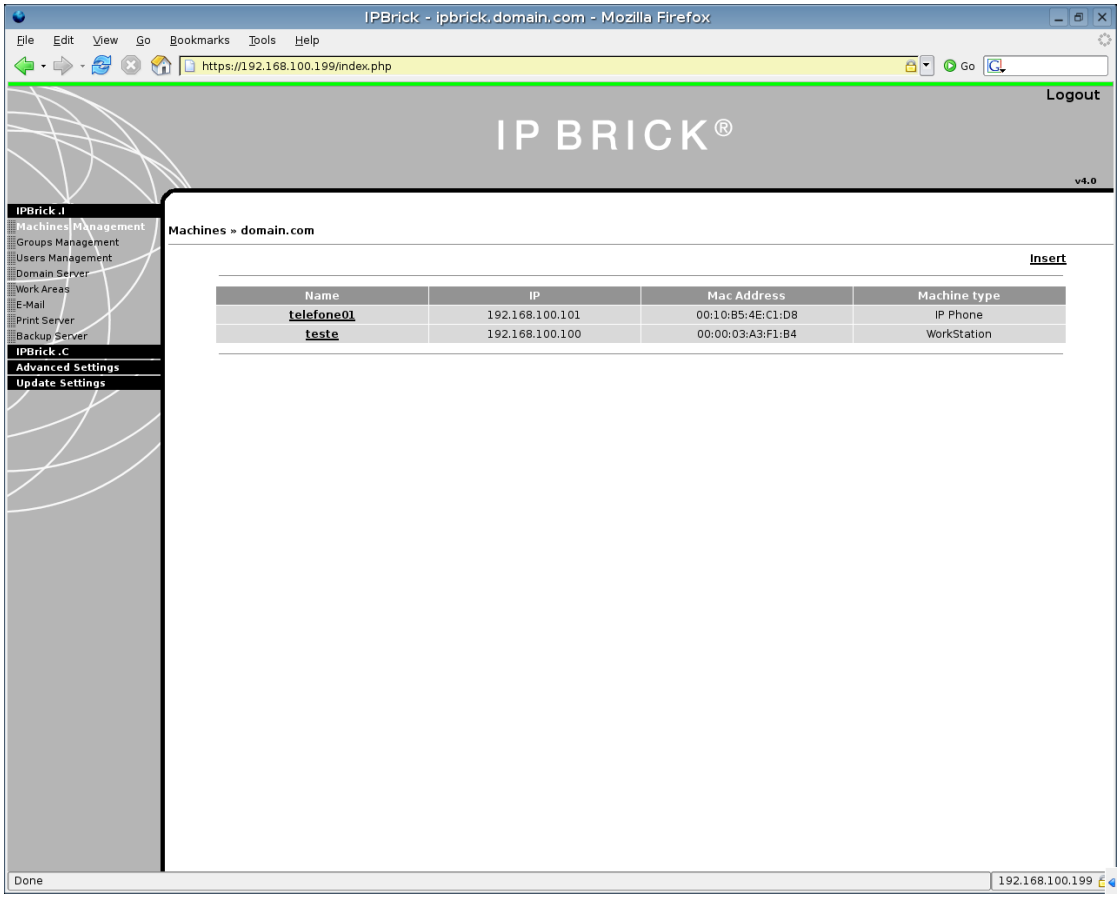

FIG. 3.1 – Gestion de Machines

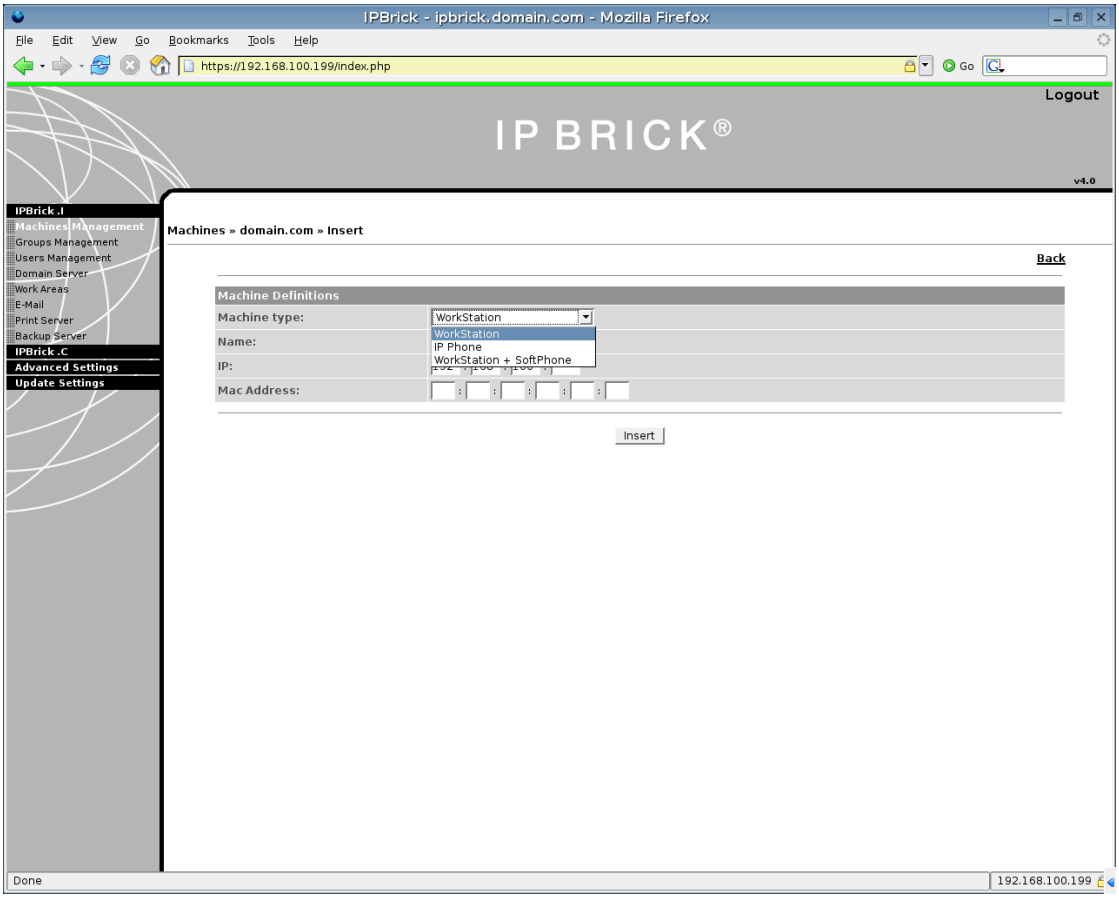

FIG. 3.2 – Gestion de Machines - Insérer

– Il ne doit pas avoir d'espaces, des caractères avec des accents ni de ponctuation. Le nombre maximum de caractères est 15 ;
– Ne doivent pas être registrées machines avec le même nom ni machines dont le nom soit le même du login d'un utilisateur registré ;
– Au cas où le registre d'une poste de travail du Windows, le nom doit être toujours rempli en minuscule et, s'il fallait, changer aussi dans le PC, le nom pour minuscule.

Les options pour Modifier et Effacer une machine sont accessibles après cliquer sur le nom de la machine dans le formulaire de la FIG. 3.1. Si on choisi `Modifier` est présenté le formulaire de la FIG. 3.3, auquel on peut redéfinir les paramètres de la machine. Si on choisit `Effacer` faut confirmer cette action dans le formulaire de la FIG. 3.4.

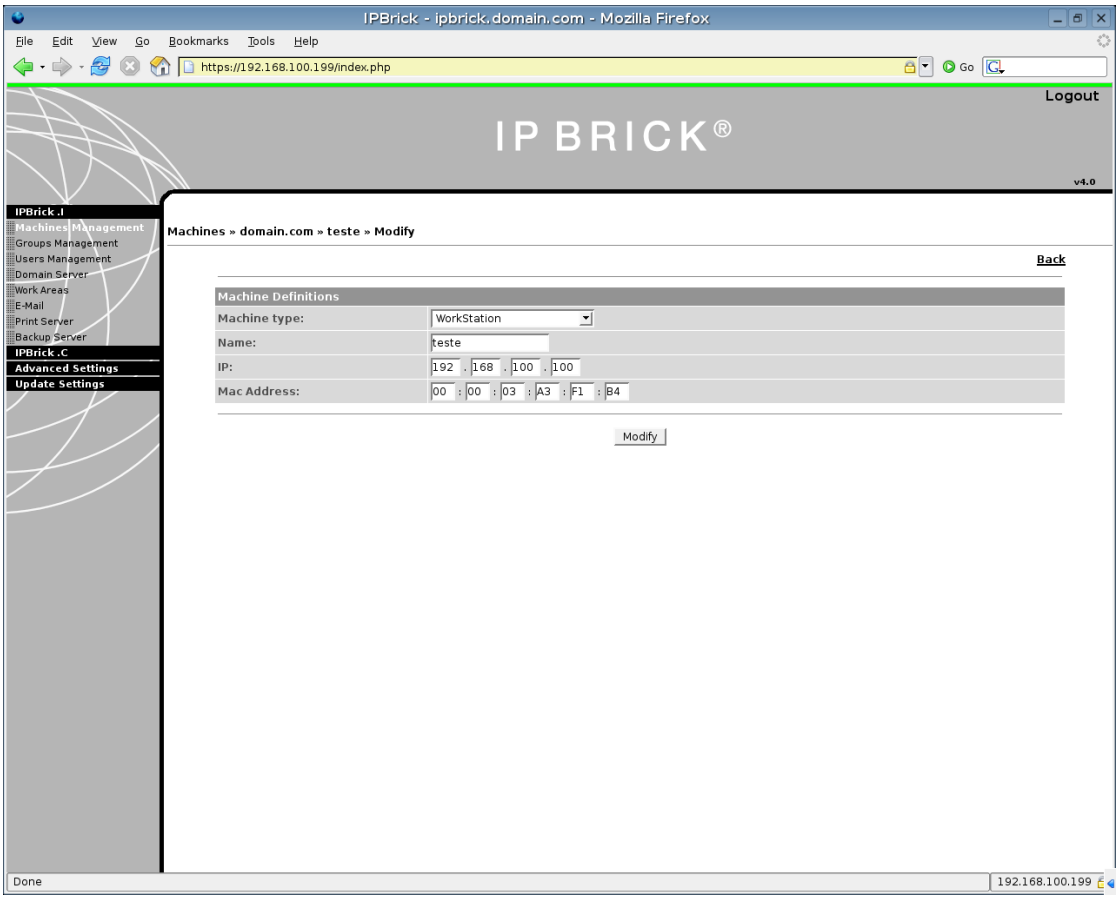

FIG. 3.3 – Gestion de Machines - Changer

3.2 Groupes

Un groupe est, essentiellement, un ensemble d'utilisateurs qui généralement est créé lorsque l'on veut que ceux-ci possèdent des autorisations communes pour un

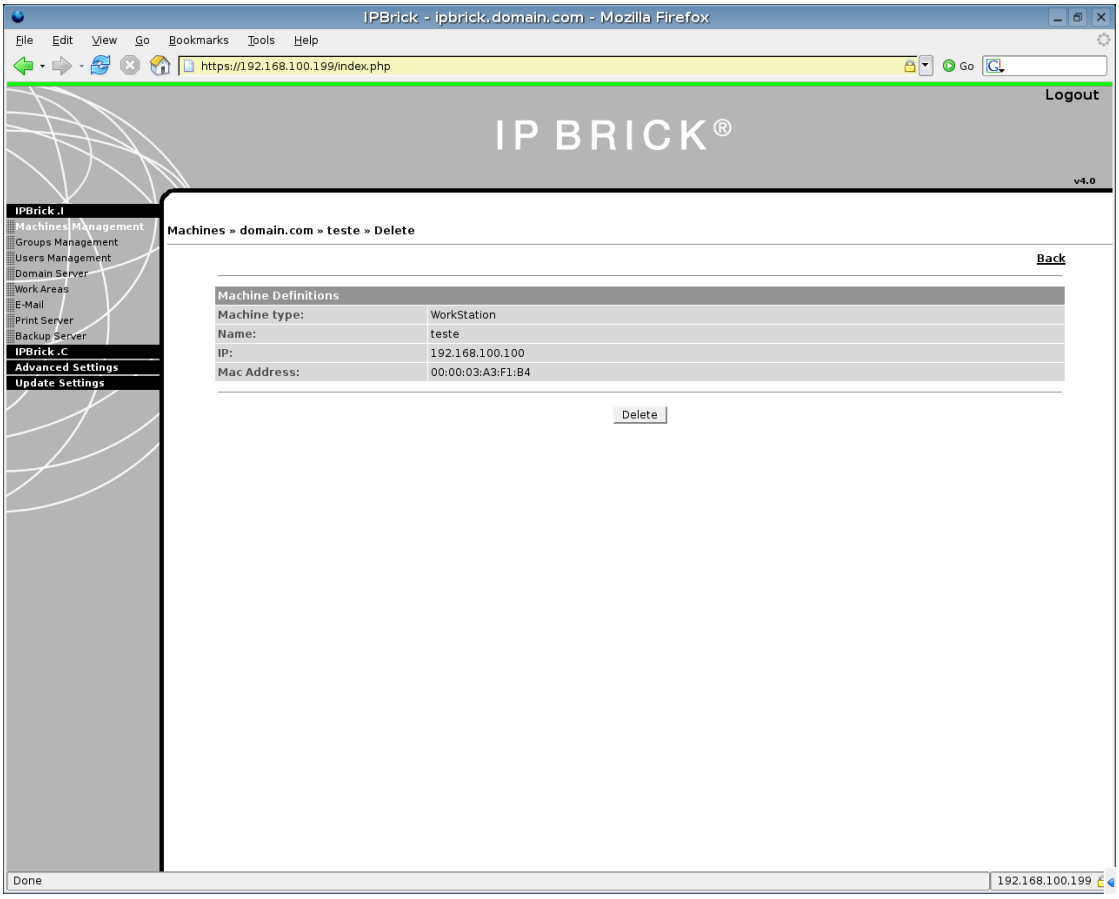

FIG. 3.4 – Gestion de Machines - Effacer

ensemble de fichiers.

Dans cette section est faite la gestion des groupes des utilisateurs dans l'*IPBrick*. Pour créer un nouveau groupe, cliquez sur `Insérer` et choisissez le nom du groupe, comme le montre l'Image Fig. 3.5. Pour ajouter ou effacer des utilisateurs d ?un groupe, cliquez tout d'abord sur le nom du groupe (Fig. 3.6) et sur la page créée (Fig. 3.7), choisissez les utilisateurs qui doivent être ajoutés ou effacés du groupe en question.

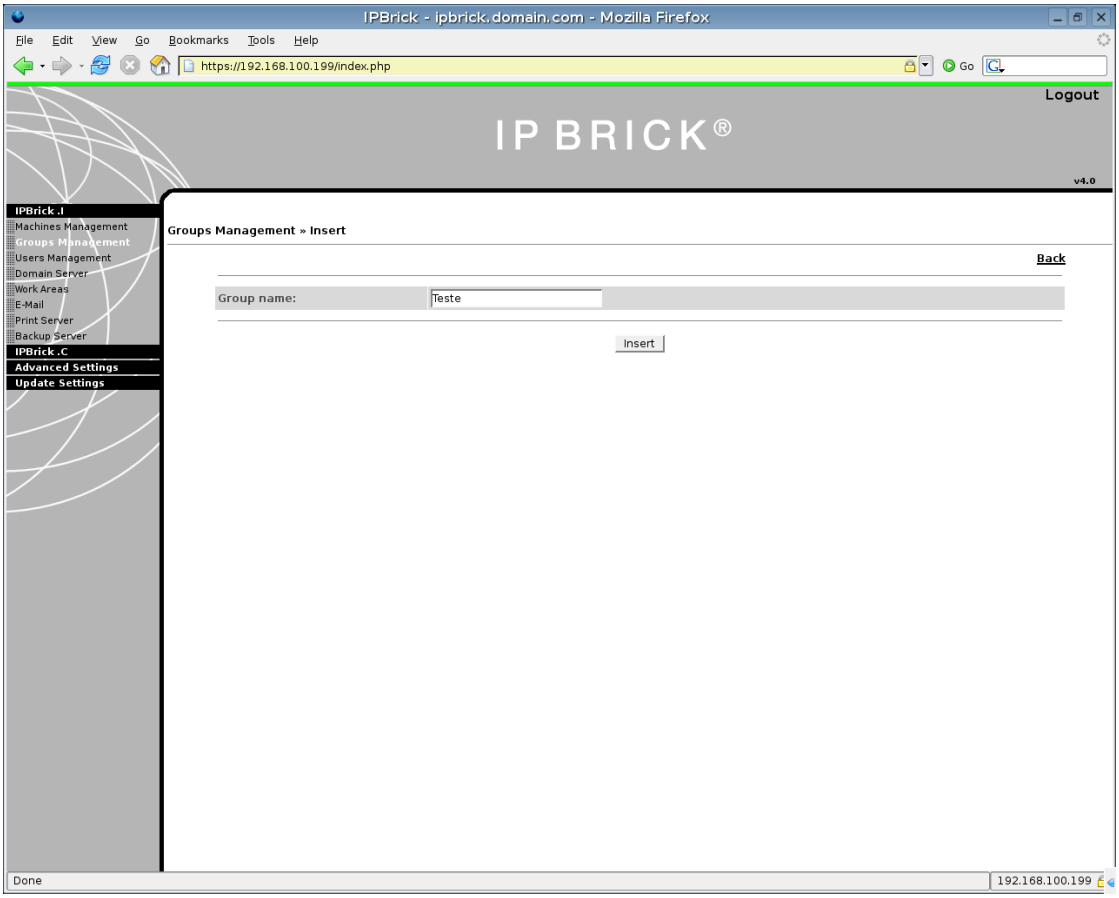

Fig. 3.5 – Groupes - Insérer

Ici sont crées nouveaux groupes d'utilisateurs, ajoutés ou retirés les utilisateurs des groupes qui existent déjà. On peut aussi modifier le nom des groupes et on peut effacé les groupes des utilisateurs. Pour modifier les caractéristiques d'un groupe, vous devrez taper dans le nom d'un groupe.

⇒ **Remarque: Il y a deux groupes prédéfinis qui ne peuvent pas être effacés ni modifiés. Ces groupes sont :**

- **Administrateurs ;**
- **Général.**

Les utilisateurs qui appartiennent au groupe des `Administrateurs` ont la permission d'administrateurs du domaine que l'*IPBrick* sert. Ils peuvent être ajoutés

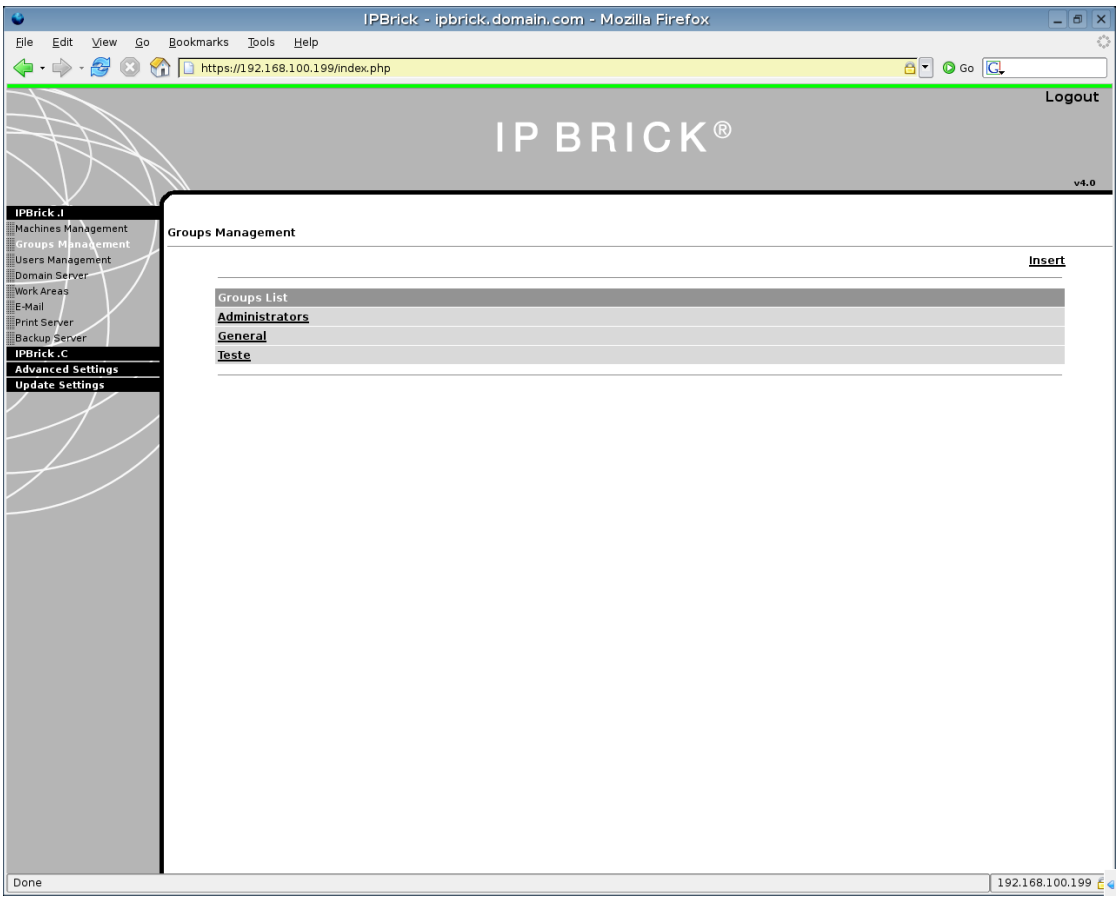

FIG. 3.6 – Groupes - Listage

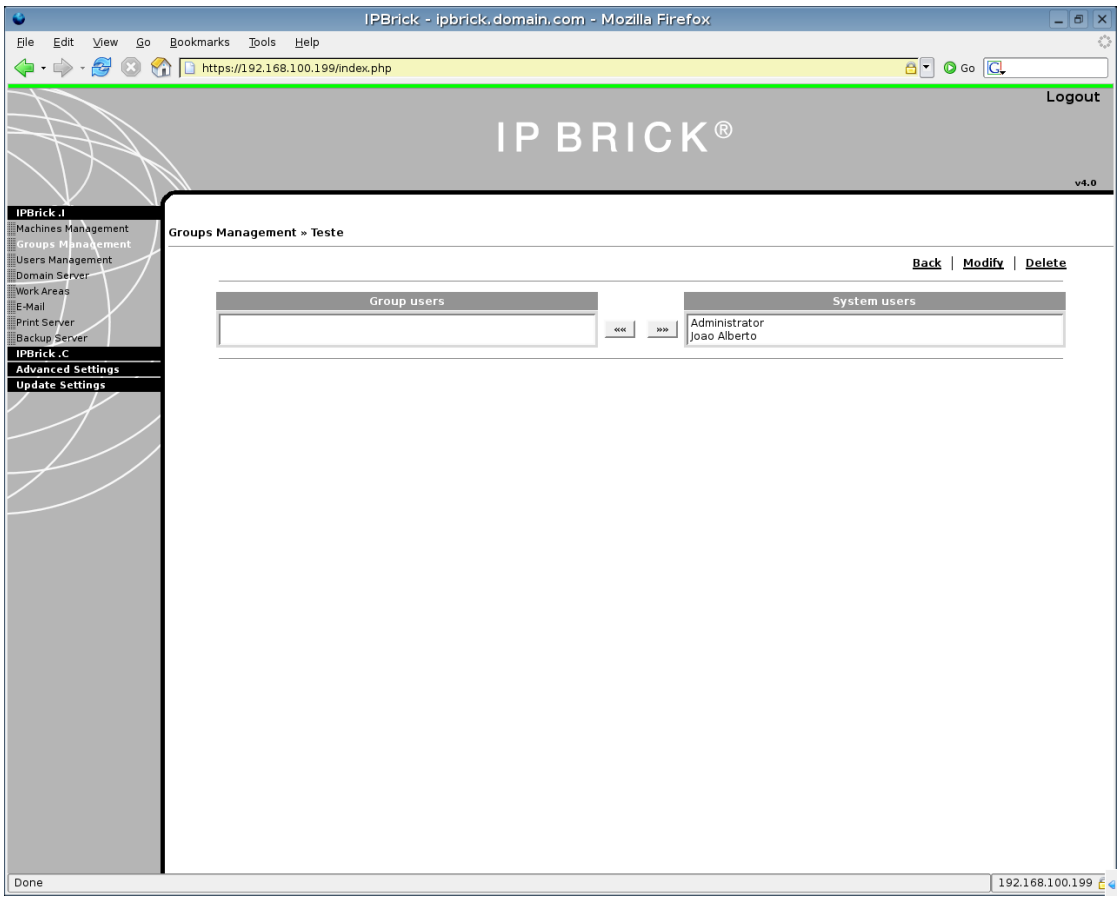

FIG. 3.7 – Groupes - Définition des Utilisateurs

ou effacés dans ce groupe, la seule exception est l'utilisateur prédéfini comme `Administrator`. Le groupe `Général` est le groupe plus commun a tous les utilisateurs crées dans l'*IPBrick*.

! Attention:
- **Quand vous insérez des nouveaux groupes, le nom du groupe peut être écrit en majuscule et/ou minuscule ;**
- **Le nom du groupe peut avoir des espaces, mais les caractères devront être alphanúmeriques, il ne peut pas avoir d'accents ni dépasser 32 caractères ;**
- **Il n'est pas possible créer groupes avec le même nom.**

3.3 Gestion des Utilisateurs

Dans cette section st possible registrer nouveaux utilisateurs, modifier l'information des utilisateurs existants et effacer les utilisateurs. Quand on crée un utilisateur, l'*IPBrick* crée immédiatement un compte de courrier électronique, un poste de travail individuel (espace en disque de l'utilisateur dans le serveur) et un *netlogon* pour l'utilisateur se légaliser dans le domaine.

⇒ **Remarque: Par défaut, après l'installation de l'*IPBrick*, seront crées un utilisateur et deux groupes. L'utilisateur crée et l'`Adminstrator` et les groupes sont `Administrateurs` et `Général`. L'utilisateur `Adminstrator` a une poste de travail 1. Cet utilisateur a caractéristiques spéciales, car il appartient au groupe d'administrateurs et il est responsable pour la gestion de quelques fonctionnalités du système, donc il ne peut pas être enlevé.**

Le registre d'un utilisateur est composé par les champs suivants :
- `Nom` : identification de l'utilisateur ;
- `Login` : identification de l'utilisateur a être utilisé pendant un processus de légalisation dans l'*IPBrick* ;
- `Serveur` : sélectionner le serveur où sera créé le compte de l'utilisateur. Le compte de l'utilisateur correspond à l'espace physique en disque, dans le serveur destiné à stocker plusieurs contenus de l'utilisateur, en inclurant la boîte du courrier électronique, le profil de l'utilisateur dans l'ambiance Windows et les documents de l'utilisateur. Au cas où il existerait serveurs esclaves ceux-ci seront aussi listés ;
- `Poste de travail` : participation physique du disque du serveur sélectionné où sera crée le compte. Vous devrez opter pour distribuer équitablement les utilisateurs de façon à profiter meilleur tout l'espace disponible ;
- `Courrier` : adresse du courrier électronique de l'utilisateur. Par défaut, il équivaut au login, si vous indiquez un autre, celui-ci sera le courrier original ;
- `Mot de passe` : définition du mot de passe ;
- `Retaper le mot de passe` : confirmation du mot de passe ;
- `Quota` : aleur pour limiter l'espace en disque que le compte de l'utilisateur pourra occuper dans le système. L'unité de valeur introduit est le Kilo bytes.

Au cas où vous n'indiquerez aucune valeur, l'utilisateur n'aura aucune limitation de l'espace occupé.
– `Validation Biométrique` : indique s'il est possible à l'utilisateur de se valider à travers de données biométriques.

! Attention:
– **Au insérer les utilisateurs, vous ne devrez pas utiliser de caractères avec des accents dans la définition du `Nom`, `Login` et `l'adresse du courrier électronique` ;**
– **Dans le champ `Nom` est possible l'utilisation de l'espace, des parenthèses, des points et les majuscules et les minuscules ;**
– **Le champ `Login` ne peut pas avoir d'espaces et vous devrez éviter l'usage des majuscules ;**
– **Chaque login doit être unique et il ne peut pas exister un login égal au nom d'une machine registrée dans l'*IPBrick*.**

Pour changer l'information qui concerne un utilisateur, il faut cliquer sur le nom de cet utilisateur (Fig. 3.8).

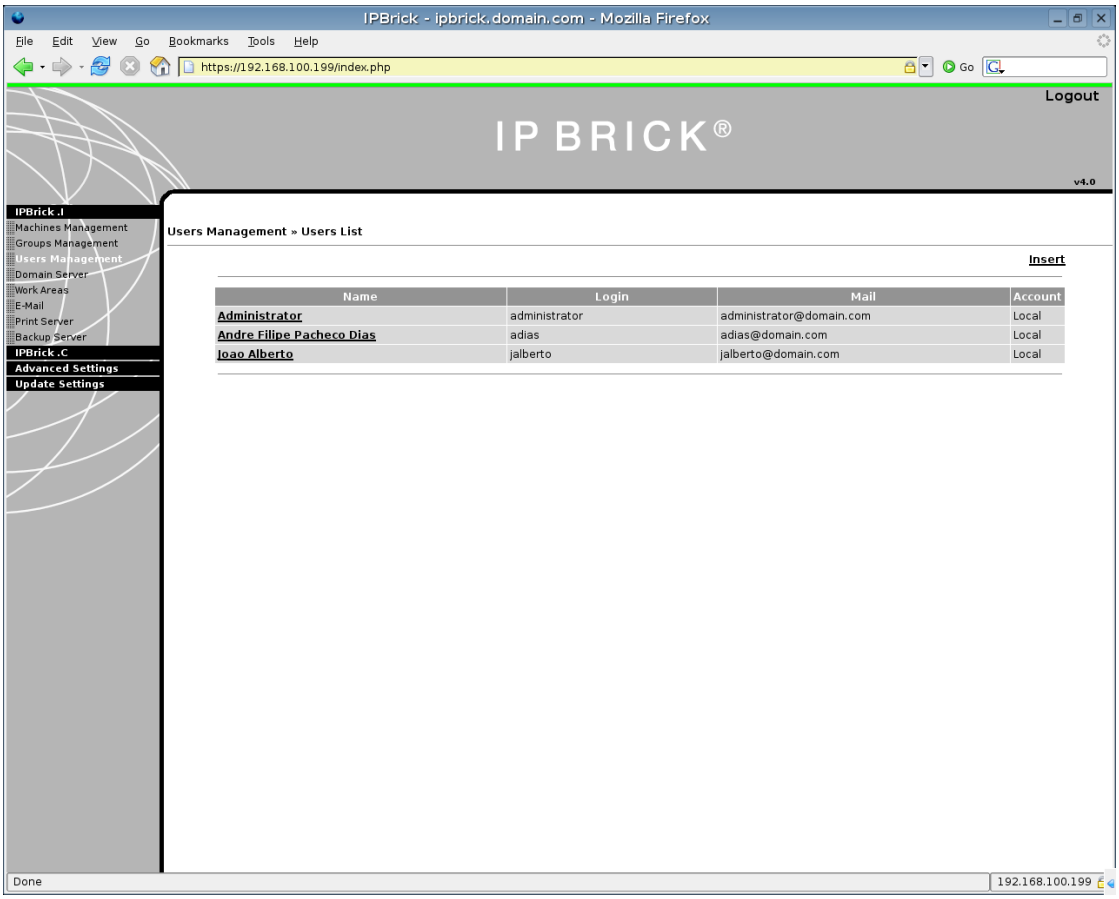

Fig. 3.8 – Gestion des Utilisateurs - Liste

Dans le formulaire pour changer les donnés d'un utilisateur (Fig. 3.11), es champs présentés sont définis pendant la création du compte de l'utilisateur. La

seule exception est l'`uidNumber`, il est le numéro d'identification de l'utilisateur dans l'*IPBrick*. Le `Mot de passe` n'est pas liste. Tous les champs définis, pendant la création d'un compte, ils sont édités, sauf les suivants : `login`, `serveur`, `poste de travail` et l'`uidNumber`.

Pour effacer le registre d'un utilisateur de l'*IPBrick*, il faut faire une clique sur le nom de l'utilisateur afin de voir les propriétés de l'utilisateur.

⇒ **Remarque: En effaçant le registre d'un utilisateur, les contenus associés a cet utilisateur (fichiers personnels, profil, messages du courrier électronique) ne sont pas écrasés. Ces contenus sont déplacés pour un partage administratif nommé Backup X (où le X représente le numéro du poste de travail où cet utilisateur est registré, 1ou 2). L'accès a ce partage est permis seulement aux utilisateurs du groupe `Administrateurs` n'importe pas le poste Windows. Pour faire ça, exécuter :**

- **Toucher [Win]+[R] au même temps ;**
- **Écrire `\\ipbrick\backupX` et toucher le bouton `OK`.**

Les dossiers et les fichiers écrasés dans ces partages administratifs sont éliminés définitivement de l'*IPBrick*.

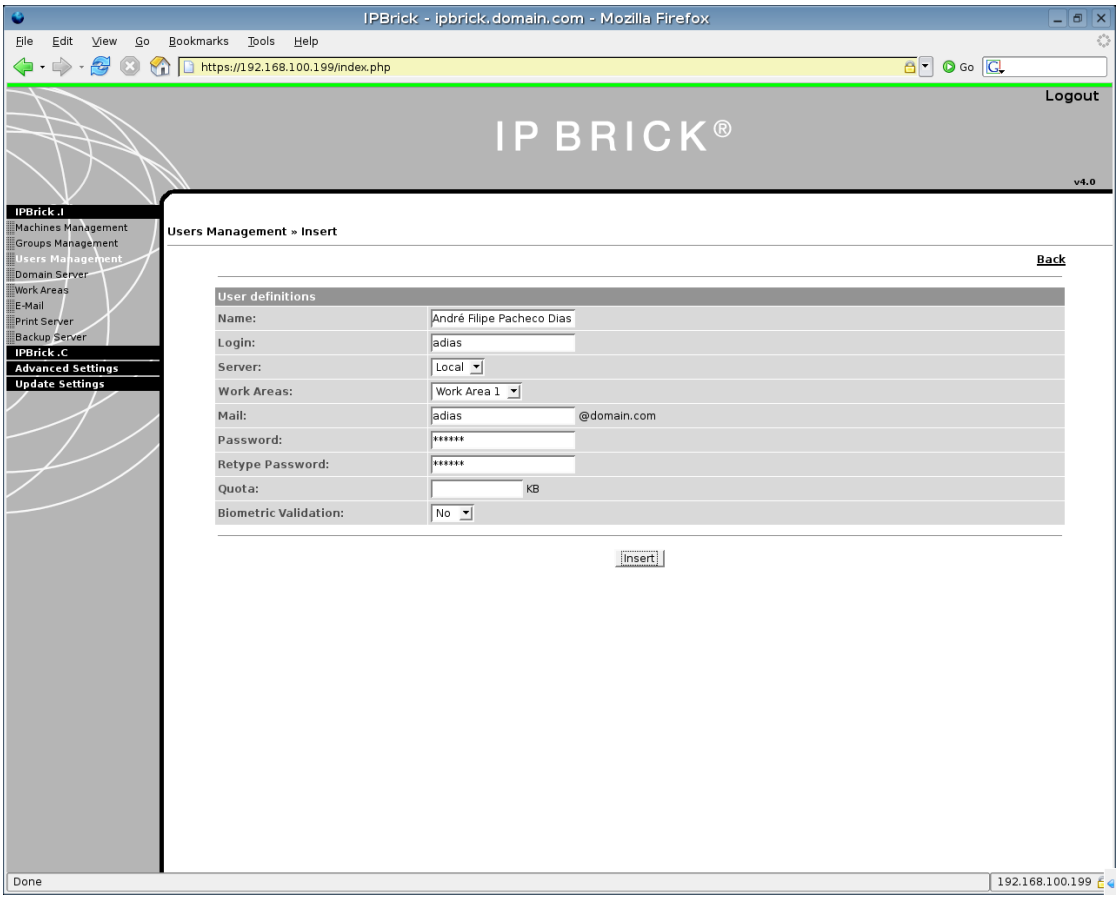

FIG. 3.9 – Gestion des Utilisateurs - Insérer

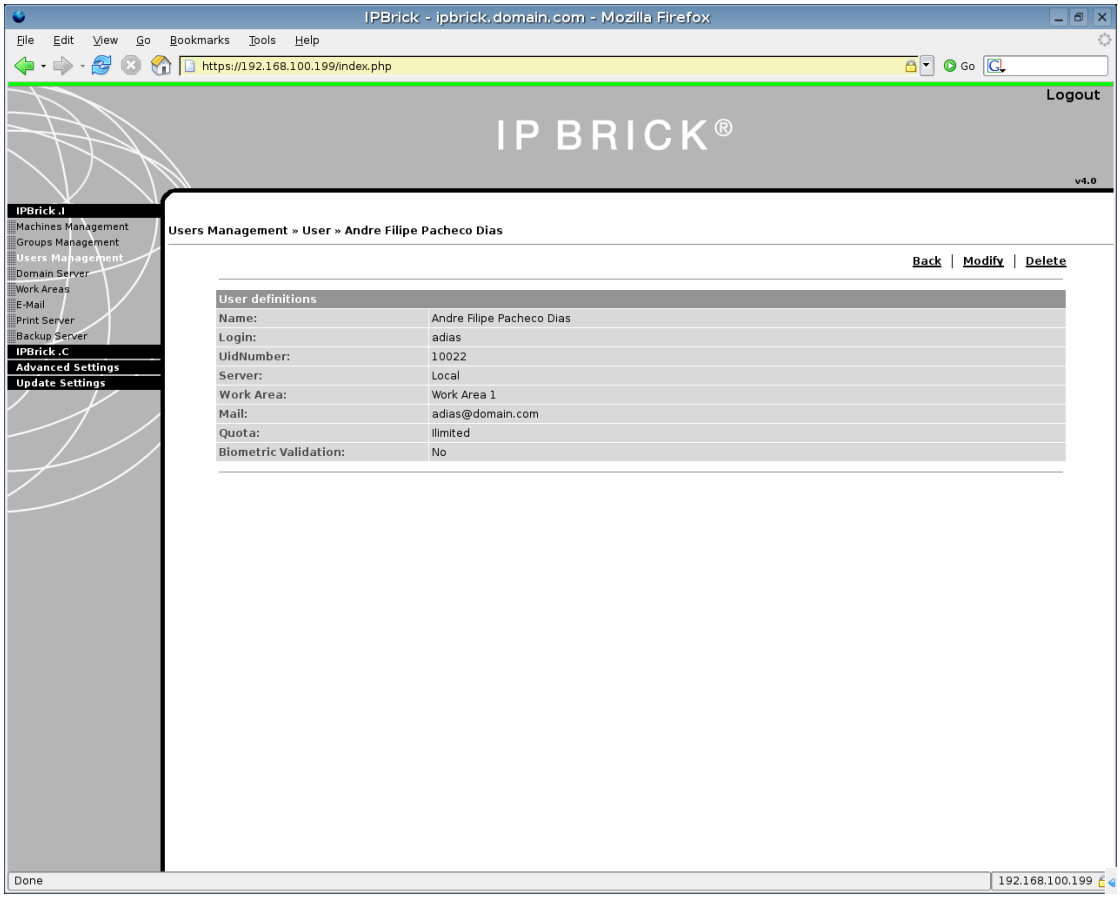

FIG. 3.10 – Gestion des Utilisateurs - Détail

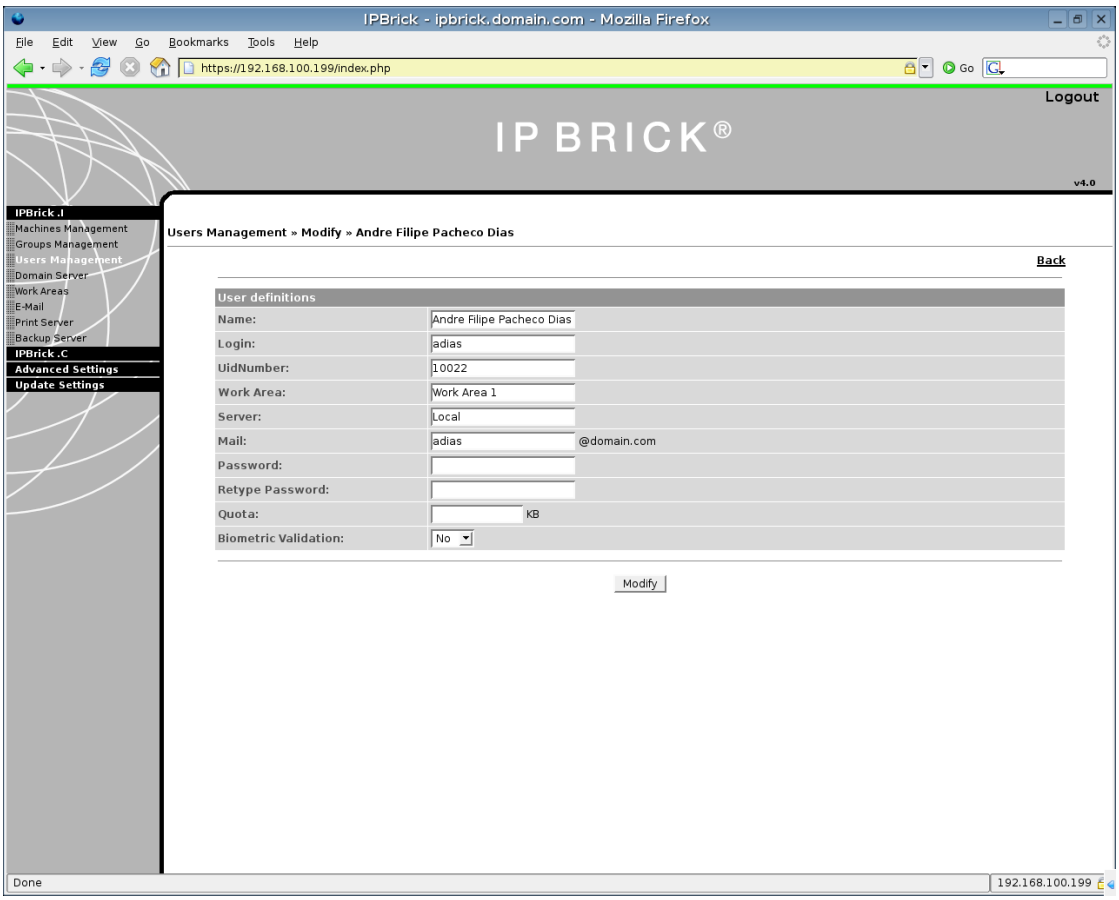

FIG. 3.11 – Gestion des Utilisateurs - Changer

3.4 Serveur de Domaine

L' *IPBrick* peut fonctionner comme un serveur de domaine (ou contrôleur de domaine), c´est-à-dire, comme un Primary Domain Controller (PDC). Le rôle d' un contrôleur de domaine est celui de gérer l' accès à un ensemble de ressources dans le réseau, comme par exemple les applications ou les imprimantes, pour un même groupe d' utilisateurs. Un domaine est identifié par un nom, et pour que les utilisateurs aient accès à ses ressources, il leur suffit d' effectuer un login dans ce même domaine.

Dans cette section est défini le nom de domaine que l'IPBrick pourra servir et le fonctionnement de l'*IPBrick* :

- `Légalisation dans le domaine=OUI` : l'*IPBrick* sera un Primary Domain Controller pour le domaine indiqué ;
- `Légalisation dans le domaine=NON` : l'*IPBrick* ne fonctionne pas commee un serveur de domaine.

⇒ **Remarque: L'information contenue dans ce page concerne l'ambiance de travail du MS Windows. Le champ Nom de domaine dans l'*IPBrick* concerne le Groupe de Travail ou Domaine dans l'ambiance MS Windows.**

3.5 Las aires de Travaux

Les aires de travaux correspondent à participations physiques du ou des disques présentes dans l'*IPBrick*. Ces participations destinées aux données des utilisateurs, elles se distribuent de la façon suivante :

1. `Les comptes personnels` : cù se trouvent les messages du courrier électronique, les fichiers e le profil de l'utilisateur dans l'ambiance MS Windows ;
2. `Partages de groupe` : destinés a stocker fichiers qui appartiennent aux groupes des utilisateurs ;
3. `Partages administratifs` : estinés a stocker les comptes des utilisateurs et les partages des groupes éliminés. Ces aires de travaux sont accessibles seulement aux `Administrateurs`.

L'*IPBrick* contient par défaut 2 `Aires de travail` : Aire de Travail 1 et Aire de Travail 2. Au cliquer sur les `Aires de travail` est présentée une liste de tous les utilisateurs et les partages du groupe organisé par l'`aire de Travail`, avec l'information d'espace occupé dans le système de fichiers, pour chaque item (Fig. 3.13).

3.5.1 Individuels

Au sélectionner les `Aires de travail` » `Individuelles` présente une liste composée par les aires de travail existantes et les taux d'occupation de chaque une. Ces aires de travail correspondent à l'espace en disque où ils sont stockés les données des utilisateurs registrés dans `Gestion des utilisateurs`.

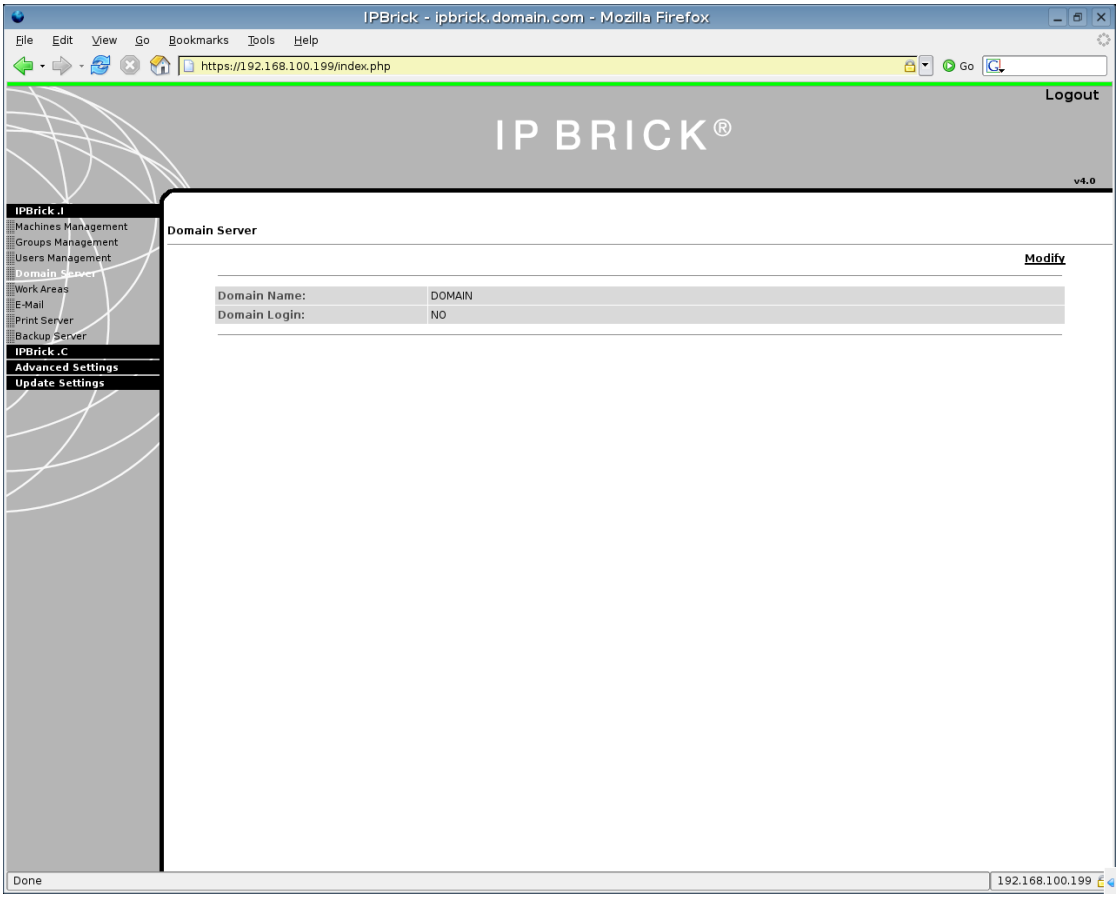

FIG. 3.12 – Serveur de Domaine

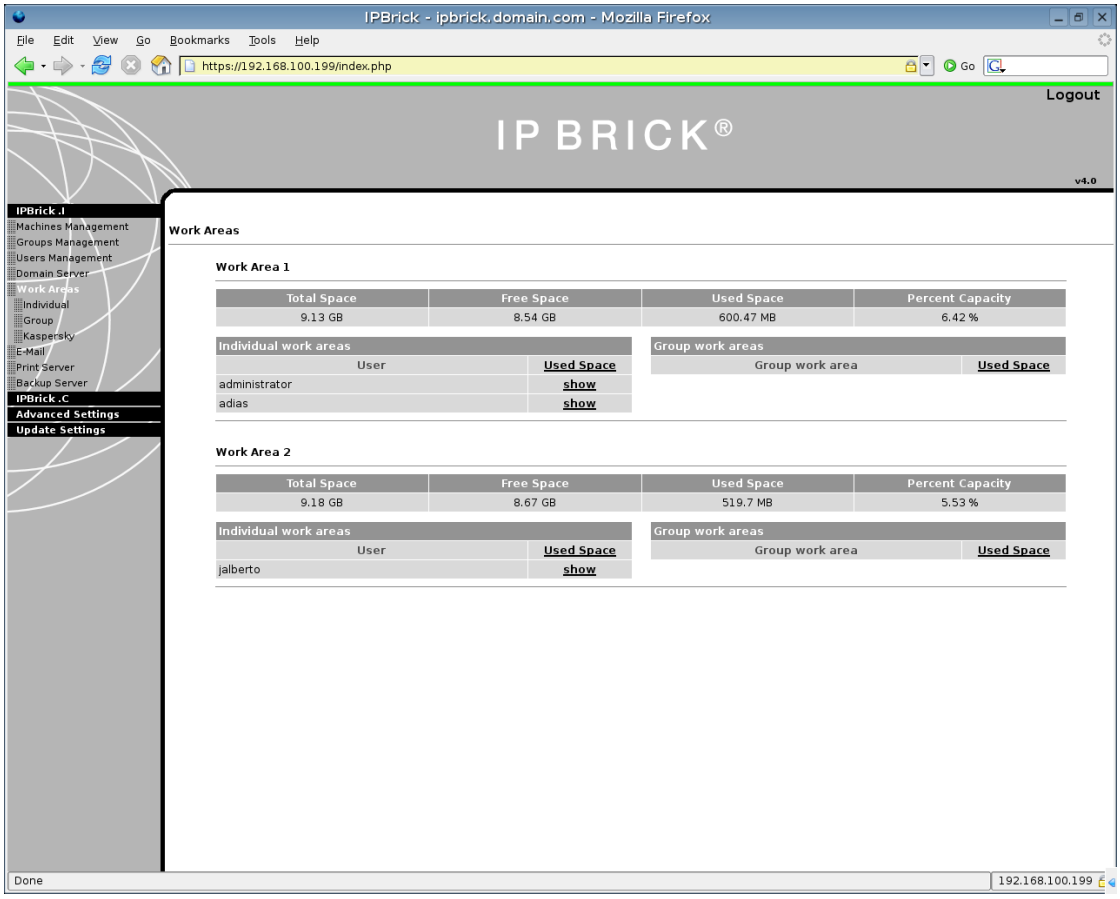

FIG. 3.13 – Aires de travail - Résumé

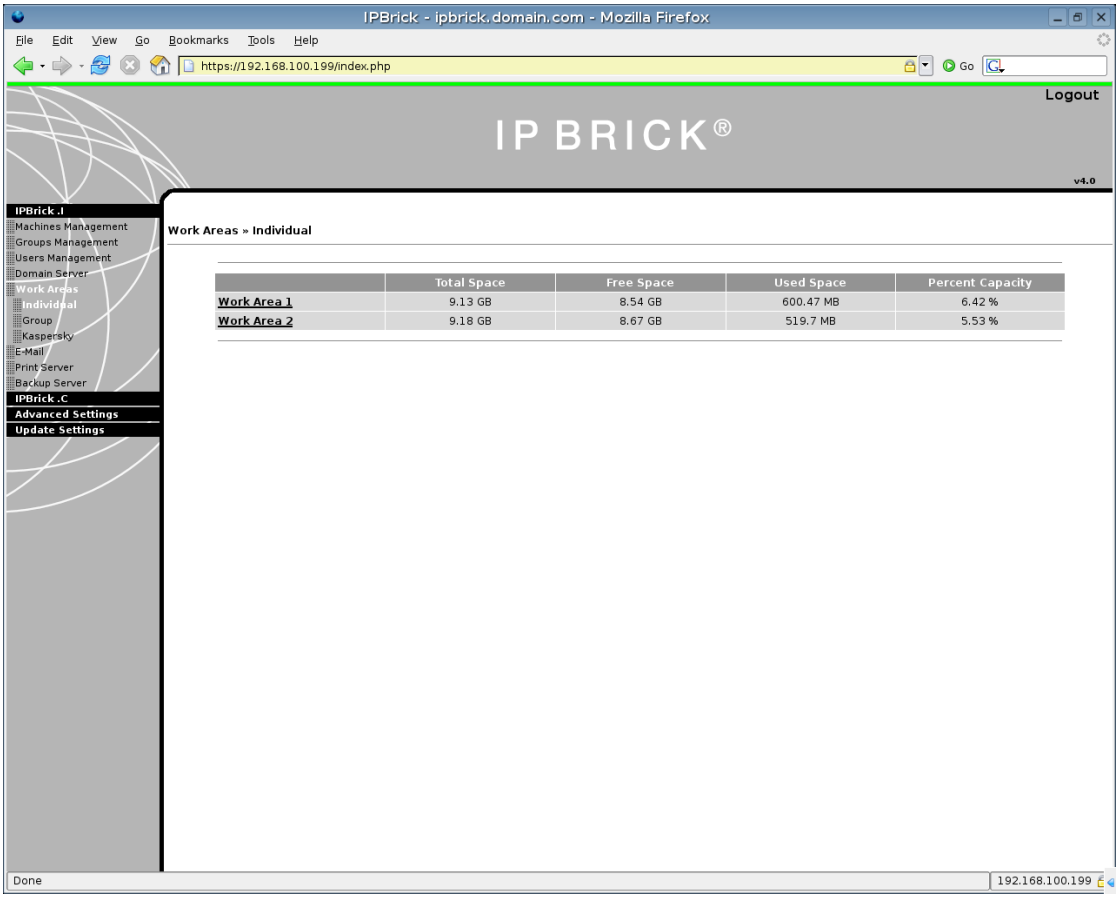

FIG. 3.14 – Aires de Travail - Résumé des Aires Individuelles

! Attention: Si l'espace disponible dans les Aires de Travail atteindre les 100%, les utilisateurs ne réussissent pas à stocker les données dans l'*IPBrick*. En plus, les messages du courrier électronique ne seront pas reçus par les utilisateurs, elles restent dans la queue d'attendre, jusqu'au moment où quelqu'un libère aucun espace dans les Aires de Travail. On conseille la manutention des taux d'occupation de chaque `Aire de Travail` avec un valeur inférieur a 95%.

Quand vous cliquez sur une `Aire de Travail`, p.e. sur l'aire de Travail 1, est présentée une liste avec tous les utilisateurs insérés dans cette aire et dans l'espace occupé pour chacun des utilisateurs. L'aire de chaque utilisateur est crée au moment où se registre l'utilisateur dans `Gestion des Utilisateurs`.

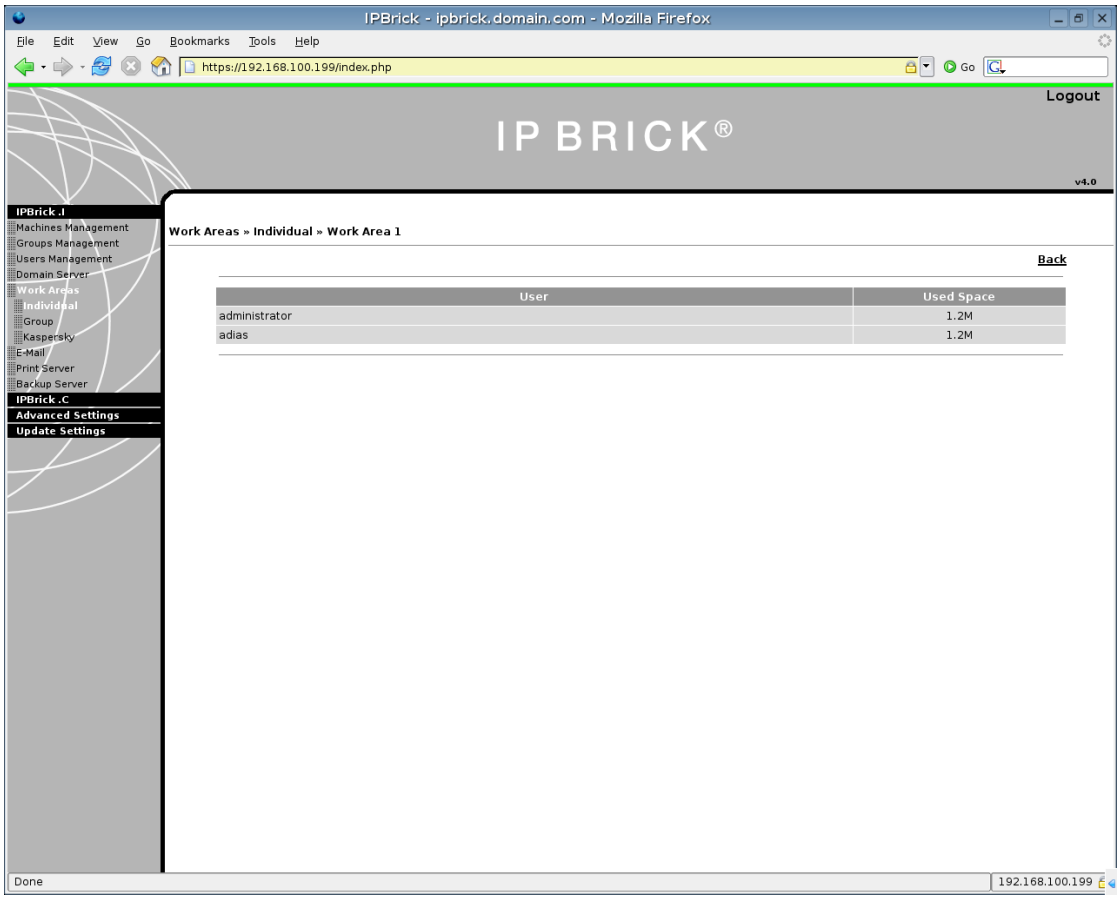

FIG. 3.15 – Aires de Travail - Individuels

3.5.2 Groupe

Les aires de travail de groupe sont des partages de réseaux (*network share*). Il est possible créer des partages de réseau en chaque aire de travail. Après créer

un partage de réseau, il faut définir les permissions d'accès pour les utilisateurs registrés dans l'*IPBrick*.

Quand vous insérez une aire de travail de Groupe, il faut remplir les champs :

- `Nom` : Nom du dossier a partager. Évitez l'utilisation des espacements, caractères accentués et de ponctuation ;
- `Description` : Informations sur le type d'utilisation qui se prétend pour ce partage ;
- `Responsable` : Ce champ n'est pas de remplissage obligatoire.

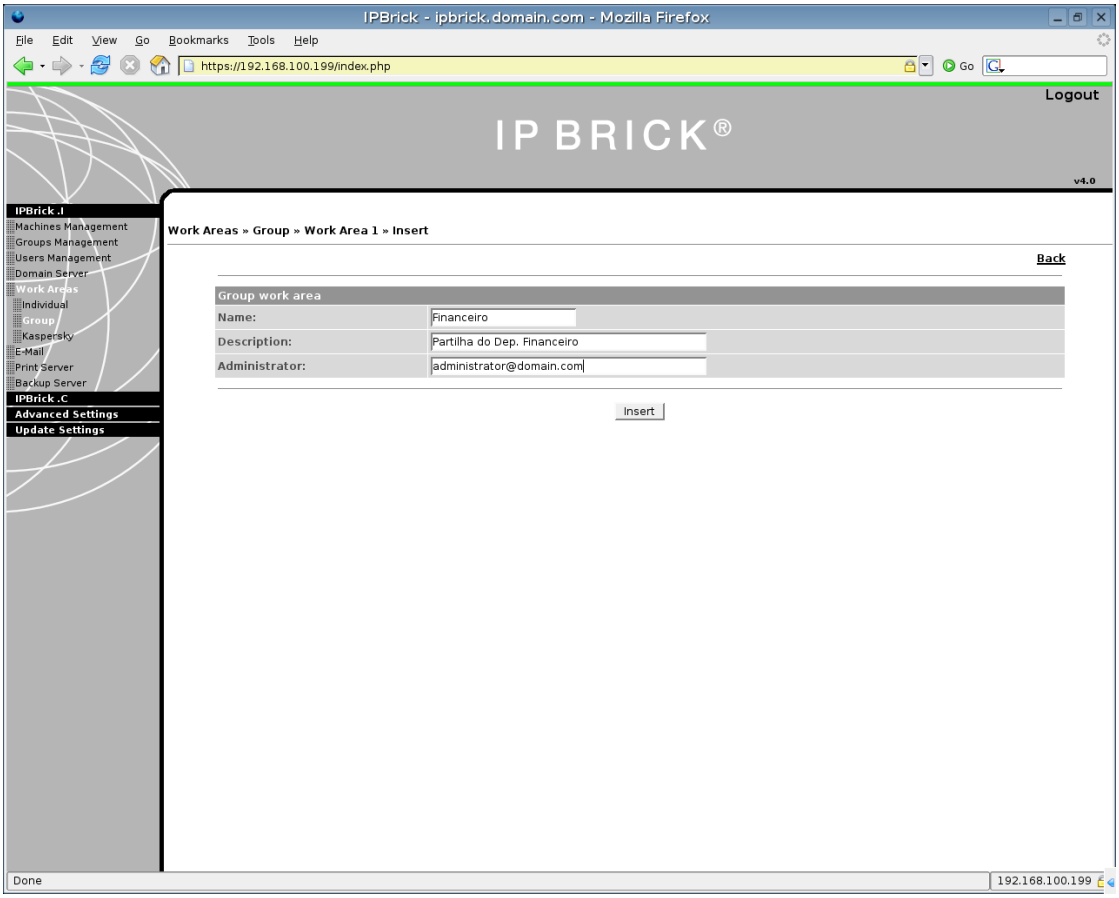

FIG. 3.16 – Secteurs de Travail - Groupe - Insertion

Groupe - Insertion Après créer un secteur de travail de groupe est nécessaire l'attribution des autorisations aux utilisateurs pour qu'ils puissent accéder au partage de réseaux. Ces autorisations sont de 3 types différents :

- Aucun : sans accès au partage. Il n'est pas possible aux utilisateurs d'ouvrir le dossier partagé à partir d'un poste de travail ;
- Seulement Lecture : les utilisateurs peuvent ouvrir le dossier partagé et les fichiers qu'elle contient. Néanmoins, il n'est pas possible de faire des modifications à ces fichiers ;

– Lecture+Écrite : les utilisateurs peuvent ouvrir le dossier partagé, accéder aux fichiers qui existent dans le partage, les modifient et garder ces altérations.

Les autorisations sont des attribués à des utilisateurs individuels ou à des groupes d'utilisateurs. Les groupes d'utilisateurs sont définis dans `Gestion de Groupes`. Par exemple, pour créer un dossier partagé pour les utilisateurs d'un département commercial la procédure serait le suivant :

– Créer le groupe "Dept_Commercial", ajouter les utilisateurs de ce département au groupe ;
– Dans `Secteurs de Travail` » `Groupe` créer un secteur de groupe "Publicité" ;
– Attribuer des autorisations de lecture et de l'écriture au groupe "Dept_Commercial". Les restants groupes restent avec des autorisations ou de la lecture ou sans l'accès.

⇒ **Remarque: Au définir les autorisations pour les groupes d'utilisateurs, quelconque modification dans le groupe Général provoque modifications pour tous les restants groupes existants. Ceci arrive parce que le groupe Général englobe tous les utilisateurs insérés dans l'*IPBrick*.**

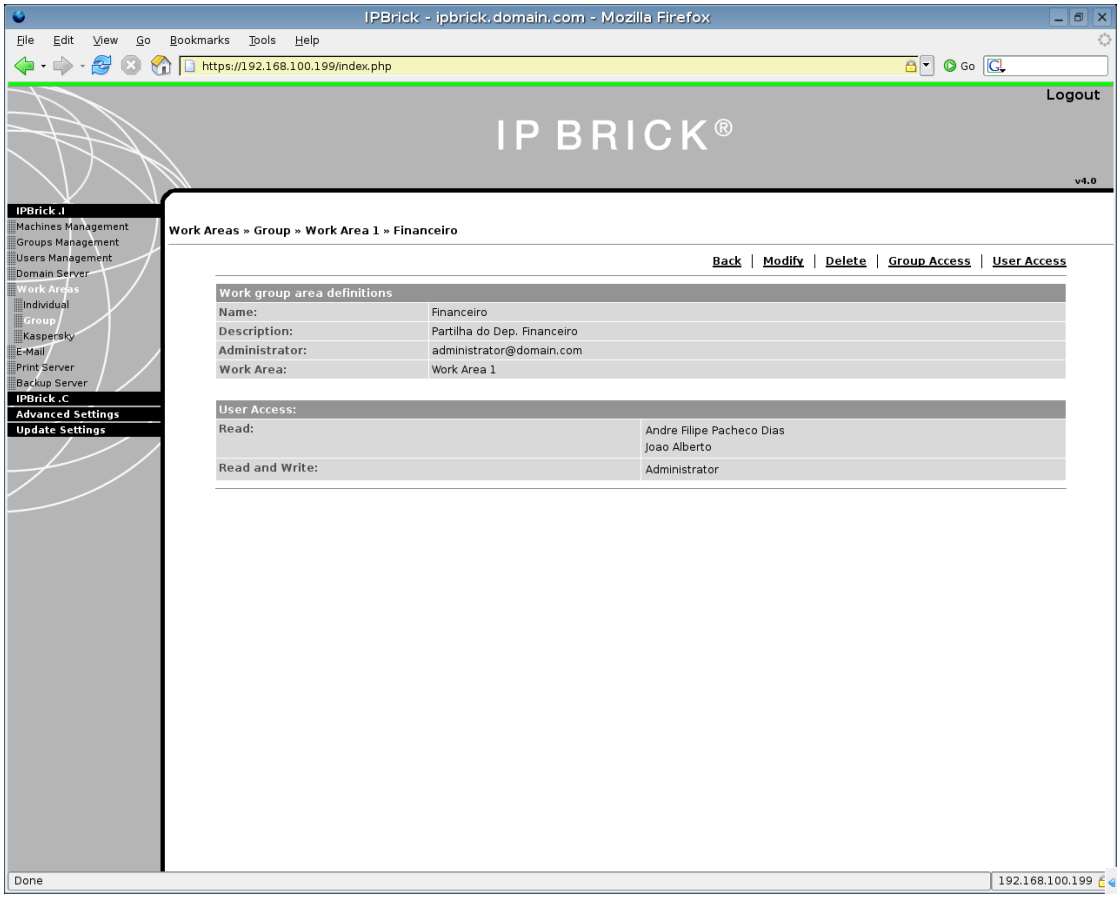

FIG. 3.17 – Secteurs de Travail - Groupe - Gestion

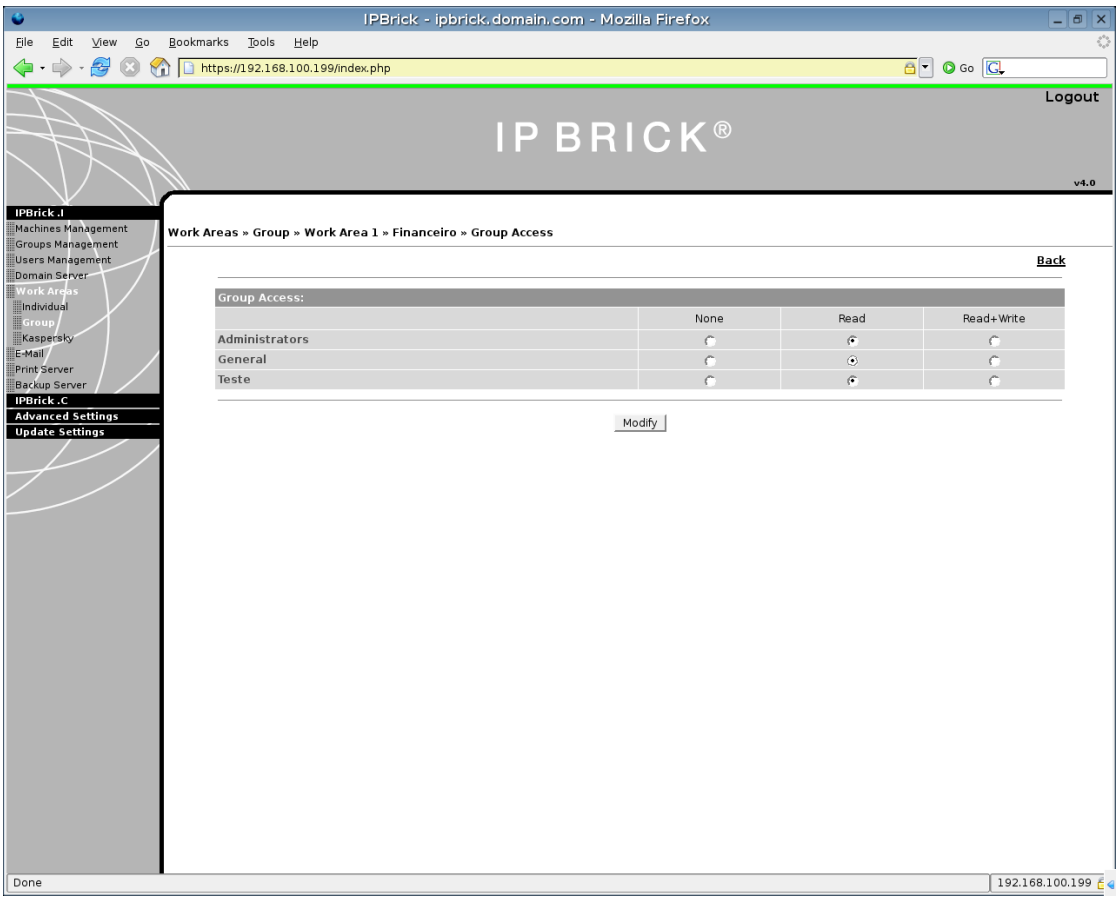

FIG. 3.18 – Secteurs de Travail - Groupe - Accès Groupes

⇒ **Remarque: Quand on efface un certain partage, ceci n'est pas disponible pour les utilisateurs. Tous les fichiers contenus dans ce partage sont déplacés pour un partage administratif appelé Backup X (où X représente le nombre du secteur de travail dans lequel ce partage a été domestique, 1 ou 2) existant dans le même secteur de travail. Ce dossier administratif seulement peut être accédé par des utilisateurs qui appartiennent au groupe d'`Administrateurs` de l'*IPBrick*. Ce partage peut être accédé à partir d'un poste Windows. Pour cela, exécuter :**

– **Taper les touches [Win]+[R] en simultané ;**

– **Écrire \\`ipbrick`\`backupX` et faire pression le bouton `Ok`.**

Les dossiers et les fichiers éteints dans ces partages administratifs sont éliminés définitivement de l'*IPBrick*.

3.5.3 Kaspersky

Le Kaspersky Antivirus pour Samba Serveurs (serveur de fichiers) já préalablement est installé dans l'*IPBrick*. Après insérer une licence valable, le Kaspersky Antivirus pour Samba Serveurs (serveur de fichiers) est actif et il est disponible une interface de gestion de l'Antivirus. (Fig. 3.19).

3.6 Courrier Électronique

Dans cette section s'effectue la configuretion du Serveur du Courrier Électronique pour utilisation dans l'Intranet, c'est-à-dire, dans le réseau local.

La section est composé par :

– Configurer ;
– Gestion de Queues ;
– Adresses Alternatives ;
– Rediriger le Courrier ;
– Réponses Automatiques ;
– Kaspersky Anti-Virus ;
– Kaspersky Anti-SPAM.

3.6.1 Configurer

Dans la `Configuretion` du courrier électronique il y a quatre concepts très simple et centraux qui conviennent se rapporter :

1. `Domaines que l'IPBrick sert` : eadresses de courrier électronique dont la destination est le serveur de l'*IPBrick*, c'est-à-dire, les comptes associés aux messages existent localement. Les messages dans la file d'attente pour traitement, au cas où ils se destinent à un de ces domaines, ils ne sont pas envoyés pour un autre serveur pour livraison. Les domaines que la machine sert, doivent aussi être correctement configurés dans le serveur de DNS de chaque domaine, c'est-à-dire, les "Serveurs de Courrier Électronique" de ces domaines doivent indiquer pour la machine ;

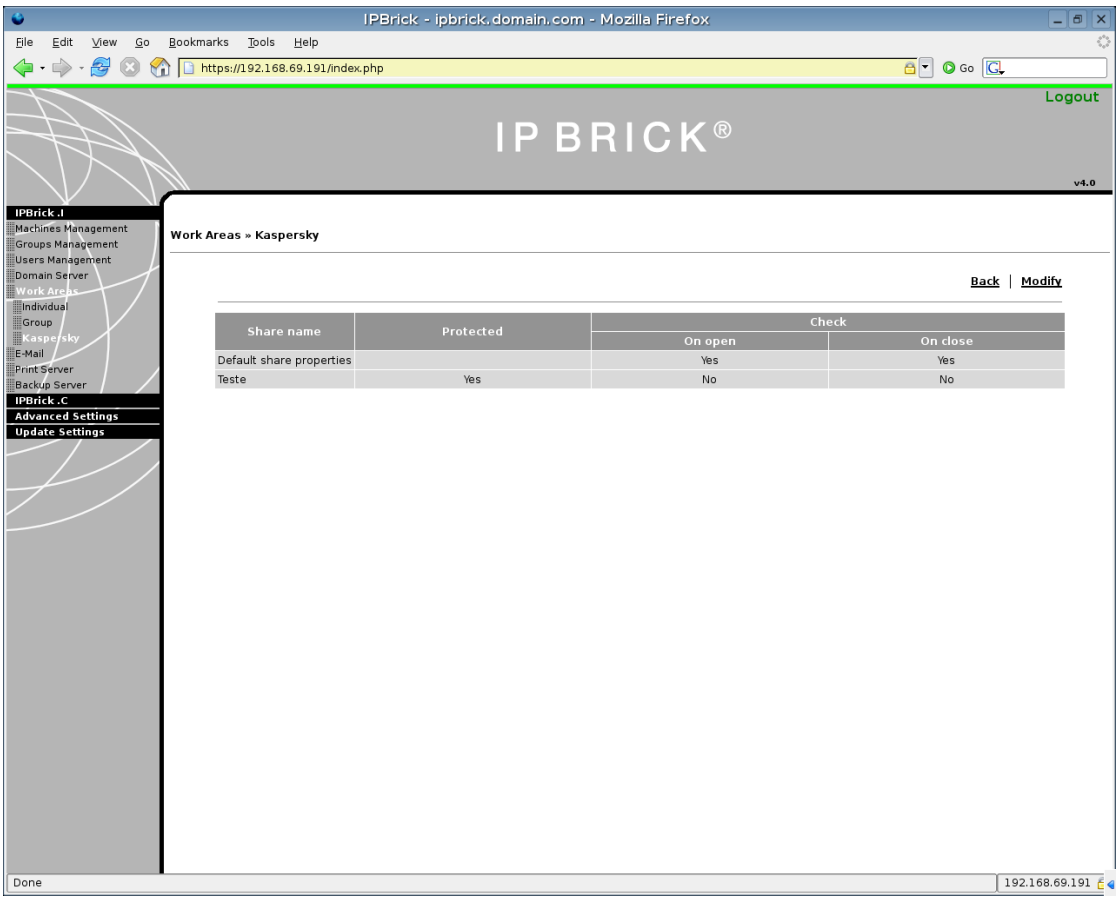

FIG. 3.19 – Secteurs de Travail - Kaspersky

2. `Domaines que l'IPBrick accepte arouteer pour le serveur de destination` : L'*IPBrick* aroutee tous les messages dont les domaines qui existent dans cette liste et que le serveur acceptera dans la queue d'attendre. Messages avec autres destinations qui ne sont pas les domaines ici indiqués ils ne seront pas acceptés par le serveur[1] ;
3. `Réseaux IP pour relais total` : L'*IPBrick* accepte faire relais pour chaque domaine dès que le message de courrier électronique soit envoyé a partir de votre réseaux interne correspondant. Au cas où il y aurait différents réseaux IP internes, il faut additionner les réseaux à cette liste, afin que toutes les machines existantes dans ces réseaux puissent envoyer les messages de courrier électronique pour les autres domaines en utilisant l'*IPBrick* comme serveur de relais ;
4. `Routes SMTP` : Les routes SMTP sont configurées quand on veut que les messages suivent un certain route (serveur) pour trouver la destination. Normalement,il est placé un serveur SMTP par défaut (en indiquant le Serveur de smtp et en laissant Domaine vide). Quand le serveur n'est pas dûment enregistré à DNS de l'Internet avec son nom et l'IP, il doit être placé un serveur de SMTP. Ce serveur doit être le serveur responsable de l'arouteement des messages de courrier électronique de l'entreprise ou du serveur de smtp de ISP utilisé par l'entreprise pour accès à l'Internet. Cette conFiguretion est nécessaire parce que certains servants de mail font des vérifications supplémentaires pour vérifier l'authenticité du serveur expéditeur. Quand ils ne réussissent pas à décider le nom du serveur pour l'adresse IP qui lui correspond au moment, le message peut être écarté ou être retourné comme suspecte de Spam. Au cas où vous n'utiliserez aucun serveur smtp, le serveur essaye d'expédier seul les messages de sa file directement dans l'Internet en faisant appel aux registres de DNS pour trouver les destinataires.

Chaque option de configuretion du Courrier Électronique a une connexion pour `Insérer` nouvelles entrées (FIG. 3.20).

Les domaines pour livraison locale (Domaines que l'*IPBrick* sert) et pour relais (dont Domaines que l'*IPBrick* aroutee) peuvent être édités et/ou éteints à l'exception de ce qui correspond au nom complet de la machine dans les domaines locales et aussi conjointement avec la domaine locale dans la relais.

⇒ **Remarque: Pour placer l'*IPBrick* à effectuer relais des messages de courrier électronique pour un autre serveur où sont logés les comptes, le domaine base de l'entreprise doit être enlevé des domaines qui l'*IPBrick* sert, vu que celui-ci est placé par défaut.**

L'*IPBrick*, par défaut, accepte seulement d'arouteer les messages de courrier électronique provenant de son réseau privé. Au cas où il y aurait différents réseaux IP internes, ceux-ci devront aussi être ajoutés, pour autoriser l'envoi de messages à partir de ces réseaux.

Il y a deux façons distinctes de définir les serveurs SMTP :

[1] Seulement les messages du courrier électronique provenant de l'internet lesquels obéiront aux règles définies, seront présentés car l'*IPBrick* n'est pas par nature configurée comme «open-relay»

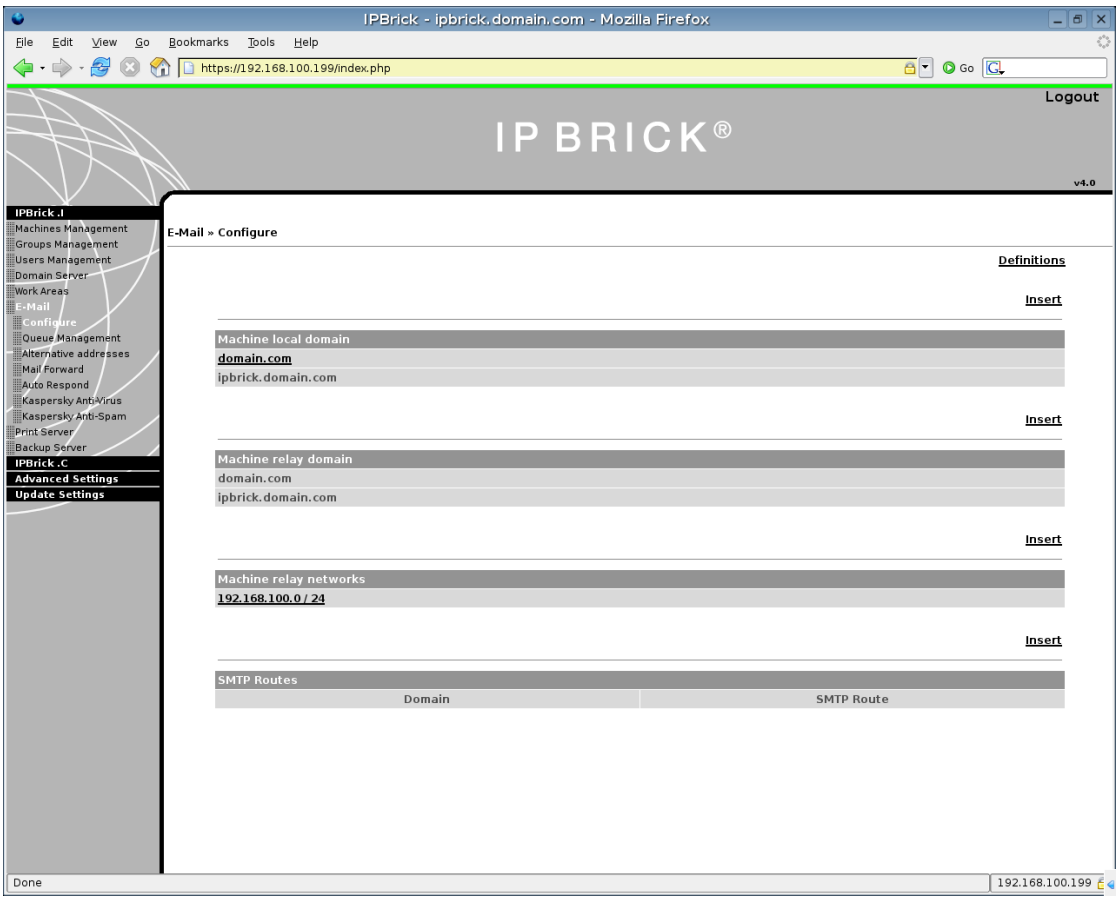

FIG. 3.20 – Courrier Électronique - Configurer

1. Nom FQDN[2] du serveur de route. P.e. : `smtp.exchange.telepac.pt` ;
2. Adresse IP du serveur de route, et maintenant il faut attenter dans la préciosité des parenthèses. P.e. : `[195.22.133.45]`.

Exemple de deux conFiguretions, une avec IP pour un domaine spécifique et l'autre pour le même domaine avec FQDN :

```
Ex.1  Domaine      : abzas.miz
 Serveur de SMTP : [195.22.133.45]
Ex.2
 Domaine      : abzas.miz
 Serveur Rota SMTP : smtp.exchange.telepac.pt
```

Une configuretion importante, s'agit de quand la machine se trouve à faire relais des messages de courrier électronique. Dans cette situation, vous devrez ajouter le serveur smtp par défaut (sans indiquer le domaine), vous devrez toujours ajouter un autre serveur de smtp pour arouteer les messages pour le serveur de courrier interne. Un exemple de cette conFiguretion est présenté à suivre, où l'*IPBrick* est en train de faire un relais pour un serveur de courrier électronique interne des comptes et elle a défini un serveur de smtp par défaut pour `smtp.isp.pt` :

```
Domaine: domain.com
Serveur SMTP: contas.domain.com
Domaine:
Serveur de SMTP: smtp.isp.pt
```

! Attention: Le serveur par défaut doit être toujours le dernier de la liste.

Définitions Il a disponibilité d'une connexion `Configuration » Définitions` (voir Fig. 3.20) qui permet définir les paramètres en ce qui concerne le serveur du courrier électronique :

- `Dimension maximum d'un message`
  Valeur par défaut : Illimité
- `Temps maximum que le serveur retient le message`
  Valeur par défaut : 604800 seconds
- `Nombre maximum de connexions SMTP simultanés`
  Valeur par défaut : 20
- `Arrêt d'entrée d'un message`
  Valeur par défaut : 1200 seconds
- `Arrêt de sortie d'un message`
  Valeur par défaut : 1200 seconds

Dans cet interface est possible définir les permissions d'envoi et réception de messages :

[2]Fully Quallified Domain Name - nom complet d'une machine qui peut être résoudre par un DNS dans son adresse IP

– `Destinataires internes valables` : Il contient la liste d'adresses de courrier électronique qui sont valables, c'est-à-dire, seulement les messages destinés a ces adresses seront acceptés dans le serveur ;

⇒ Remarque: Du moment où vous insérez les destinataires internes valables, seulement les adresses ici existants reçoivent les messages.

– `Expéditeurs invalides` : Il contient la liste d'adresses de courrier électronique lesquels ne sont pas autorisés a envoyer messages.

3.6.2 Gestion de Files d'attente

La gestion des files d'attente ((Fig. 3.21) permet la gestion et le visionnement des messages qui sont dans la queue du serveur du courrier électronique afin d'être livrer au destinataire, soit locale ou éloigné.

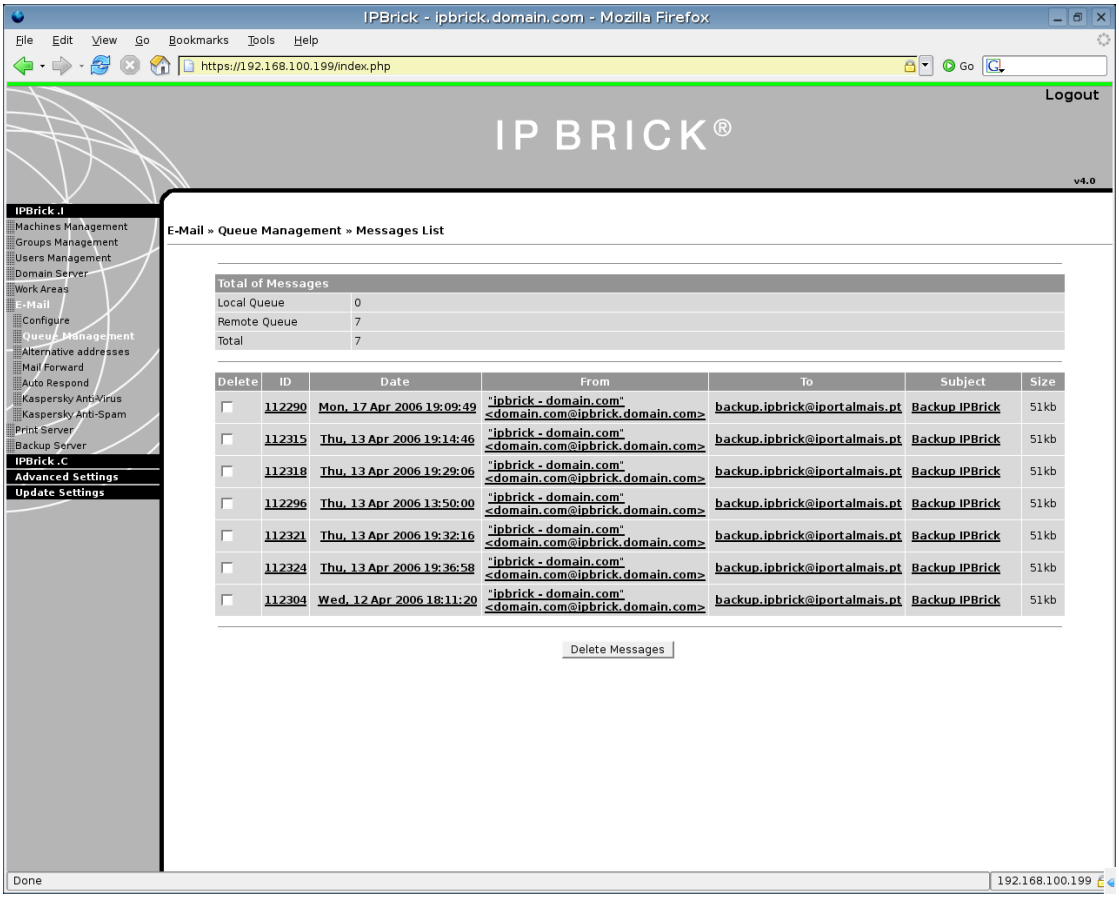

Fig. 3.21 – Courrier Électronique - Gestion de files d'attente

Vous pouvez consulter le nombre des messages en file d'attente pour les destinataires locales ou éloignés et aussi le nombre total. Dans la liste des messages existants dans la queue seront présentés les champs suivants :

- `ID` : seul identificateur du message ajouté par l'*IPBrick* ;
- `Date` : Date du envoi du message ;
- `De` : Expéditeur du message ;
- `Pour` : Destinataire du message ;
- `Volume` : volume du message présenté en Kbytes ;

Il y a la chance d'effacer plusieurs messages au même temps, en sélectionnant les *checkboxes* respectives et cliquant dans l'option `Effacer Messages`. Il vous est demandé la confirmation pour l'élimination des messages sélectionnés.

! Attention: Es messages éteints de la file d'attente seront définitivement éliminés !

Quand vous sélectionnez un message, vous pouvez voir la source complète de la même. Cette opération est faite dans temps réel, il ne faut pas faire Mettre à `Jour des Définitions`.

3.6.3 Adresses Alternatives

Les adresses alternatives (Fig. 3.22) sont une forme d'avoir d'une part logins praticiens et faciles de gérer et d'autre part, le confort d'utiliser des adresses de courrier électronique plus personnalisées. De cette forme, l'utilisateur peut avoir une adresse de courrier électronique avec lequel s'identifie mieux. Toutes les messages avec destination à une des adresses alternatives définies pour un utilisateur sont livrées dans la boîte de courrier respective.

```
Ex.  nom  : Armindo Quintas
       login : aquintas
       email : aquintas@domain.com

       emails alternatives:
         armindo_quintas@domain.com
         armindo.quintas@domain.com
         armindo@domain.com
         comercial@domain.com
```

Pour `Insérer` une nouvelle adresse de courrier doit sélectionner ce que le compte (utilisateur) où prétend définir une adresse alternative et introduire la nouvelle adresse de courrier électronique.

Chaque fois que soit prétendu, vous pouvez accéder à la liste d'adresses (qu'est commandé par utilisateur de l'*IPBrick*, avec leurs adresses de courrier électronique regroupées) et modifier une certaine adresse pour une autre désignation ou pour une autre utilizador[3].

[3]Comme il est évident lors du changement d'une adresse alternative d'un utilisateur pour autre, celui-ci autre reçoit seulement les nouveaux messages tandis que les anciens continueront dans le compte de l'ancien titulaire.

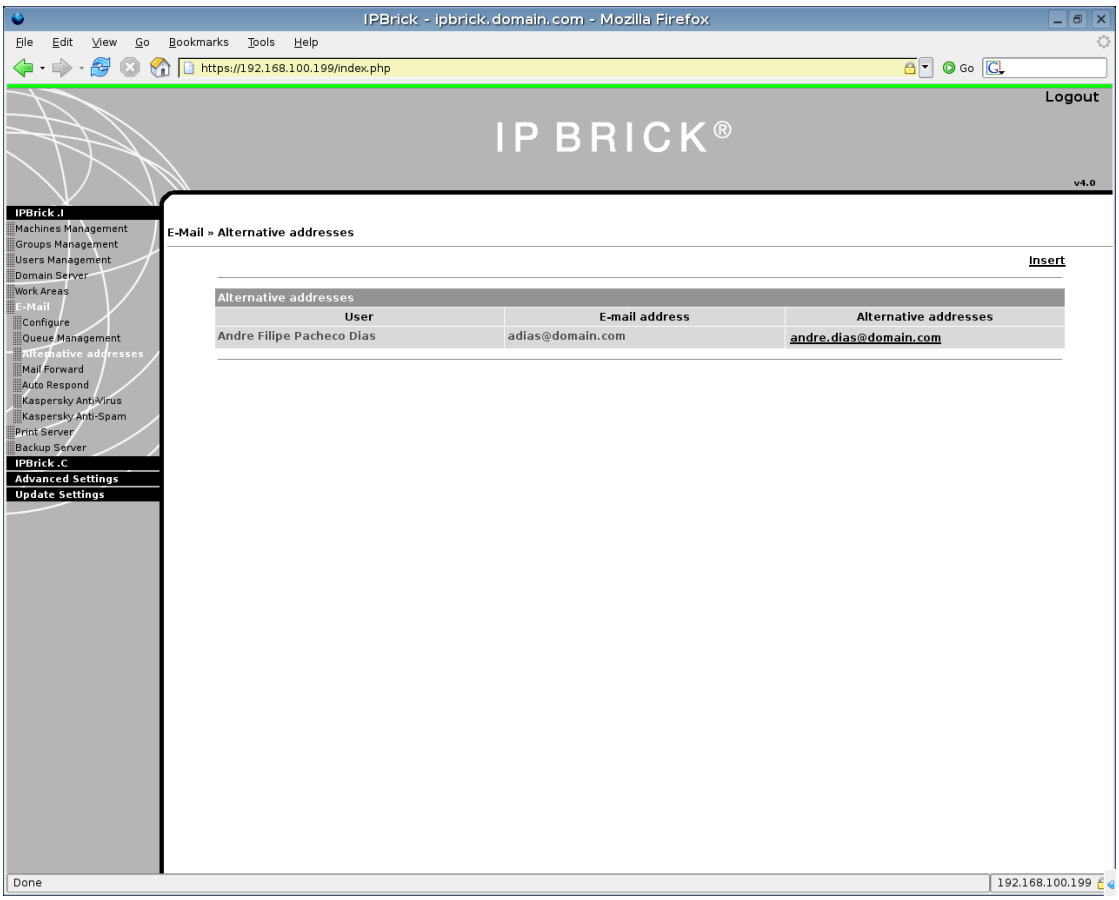

FIG. 3.22 – Courrier Électronique - Adresses Alternatives

3.6.4 Guider le Courrier

L'arouteement de courrier électronique permet que les messages livrés dans une certaine boîte de courrier puissent aussi être arouteés pour autres boîtes de courrier, ils peuvent être internes ou externes (FIG. 3.23).

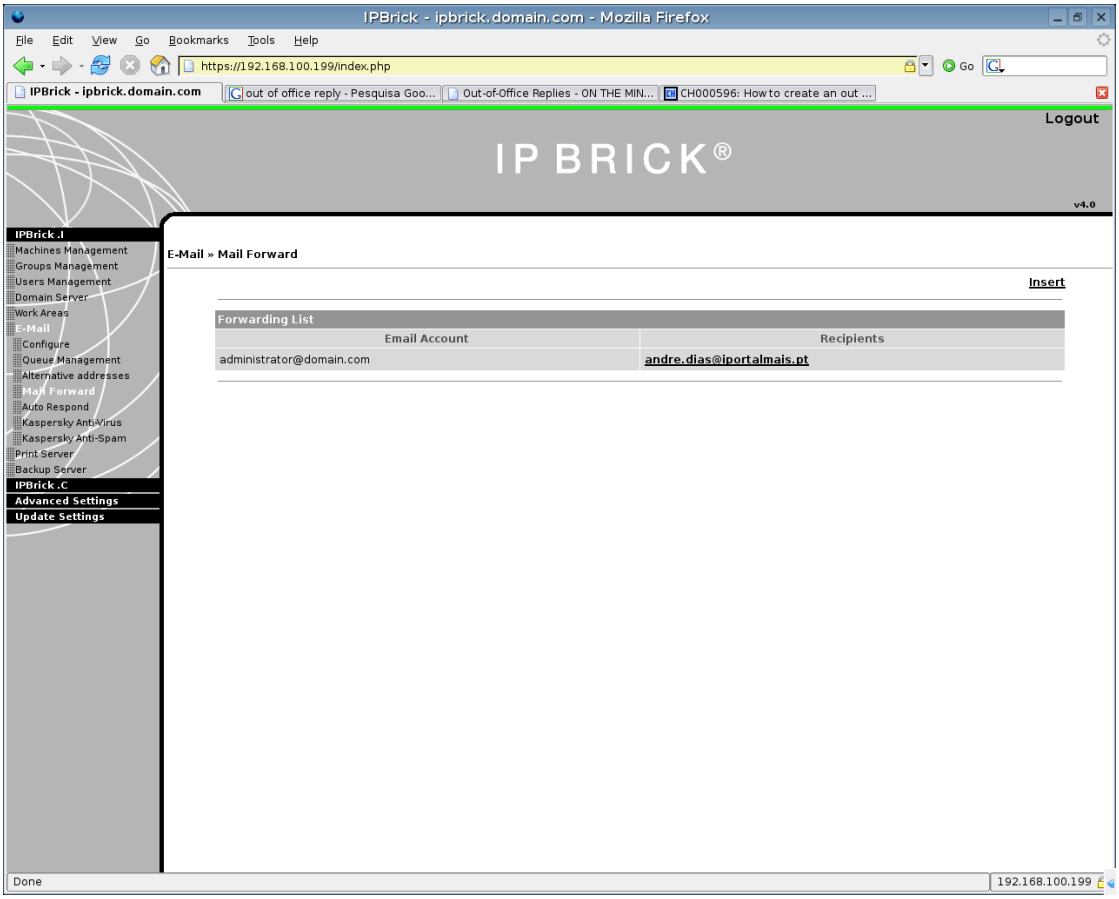

FIG. 3.23 – Guider le Courrier

Pour `Insérer` un nouvel arouteement (FIG. 3.24) doit sélectionner le compte de courrier local où prétend activer l'arouteement des messages et définir l'adresse destination pour laquelle les copies de ces messages seront envoyées. Il est mis à la disposition une liste commandée et regroupée par les adresses locales de l'*IPBrick*, dans laquelle, à travers la sélection d'un des récipients de destination, vous avez la possibilité de `Modifier` ou d'`Effacer` cette entrée.

3.6.5 Réponses Automatiques

Une Réponse Automatique est un message de courrier électronique envoyé automatiquement par l'*IPBrick* dans réponse à un autre message. Quand un message arrive au compte d'un destinataire qui a une Réponse Automatique configurée, l'*IPBrick* envoie un message pour l'expéditeur de la même, avec un contenu personalisé par l'utilisateur. Pour `Insérer` une nouvelle Réponse Automatique, vous

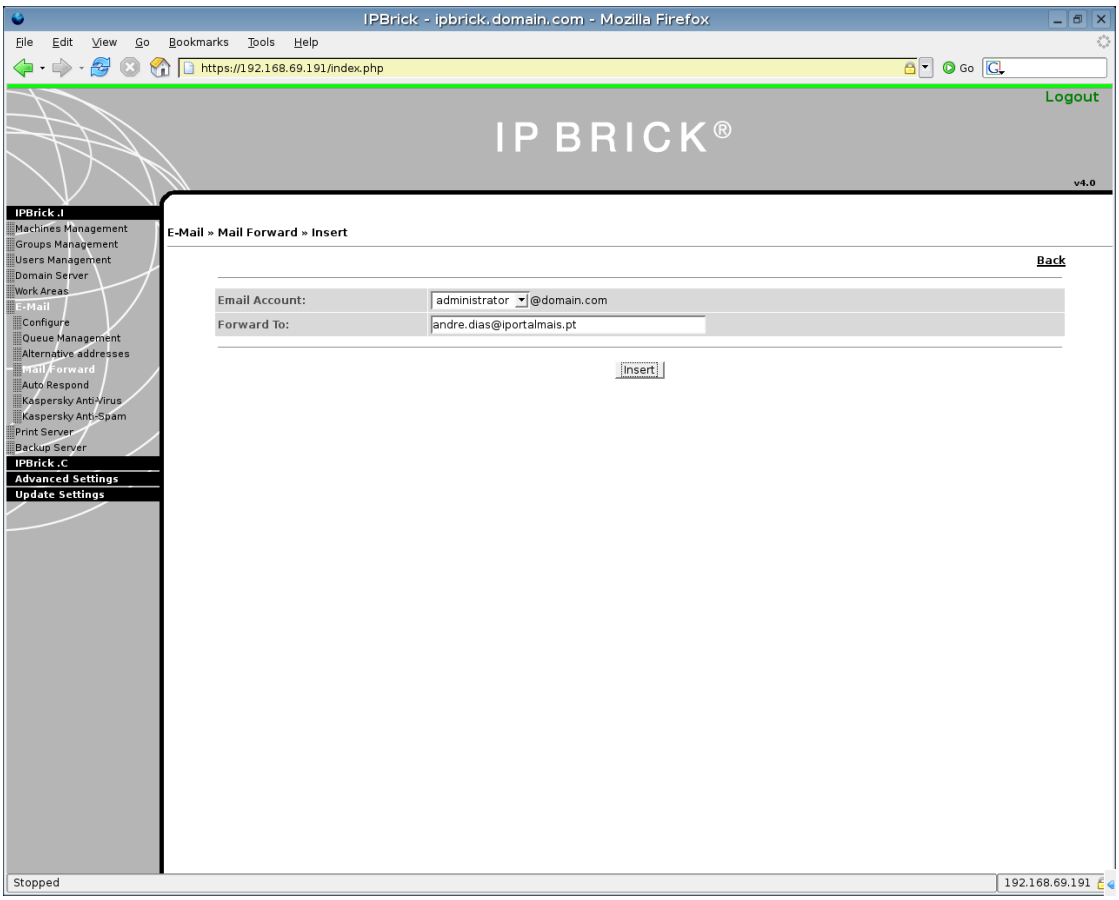

FIG. 3.24 – Guider le Courrier - Insertion des comptes

devrez sélectionner le compte de courrier électronique prétendu et la textarea existante introduire le message de texte qui sera envoyé dans le message de réponse automatique. Un exemple typique de création d'un message automatique est présenté dans la Fig. 3.25.

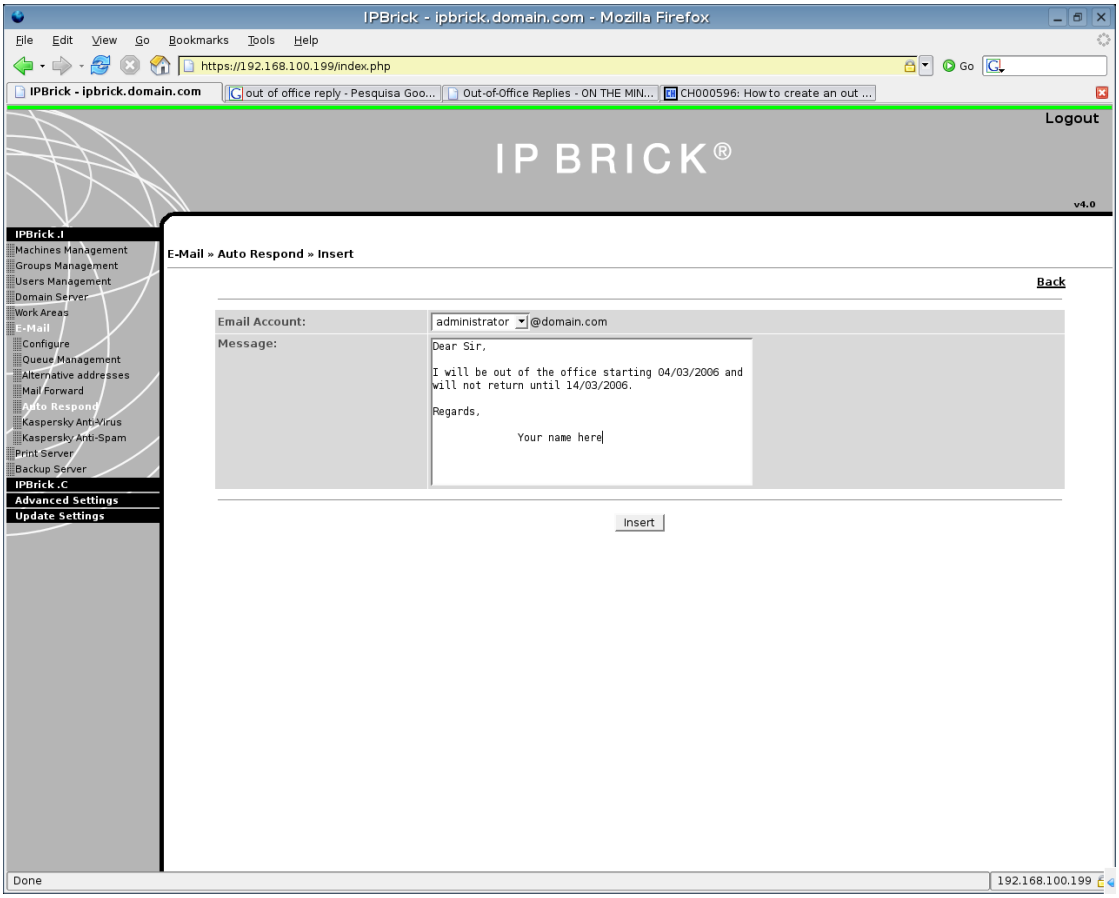

Fig. 3.25 – Courrier Électronique - Réponses Automatiques

Il est mis à disposition la liste ordonnée et agroupée par les adresses locales de l'*IPBrick*, dans laquelle, en sélectionnant un adresse de courrier électronique, vous pouvez `Changer` ou `Effacer` cette entrée.

3.6.6 Kaspersky Anti-Vírus

Dans la section de courrier Électronique, il y a déjà l'Antivirus pour courrier Électronique pré installé. Seulement c'est nécessaire d'acquérir une licence pour activer son interface de gestion. Le même arrive avec le Kaspersky Anti-SPAM, également pré installé. Dans une section plus (4.4.3) en avant nous tournerons au Kaspersky.

3.7 Serveur Imprimante

Dans cette section, il est mis à la disposition l'interface de gestion des imprimantes qui se prétendent mettre dans le réseau. Quand vous avez la chance de définir une imprimante, sont demandés plusieurs paramètres :

1. `Nom` d'imprimante (Ex. : HP2200) ;
2. `Description` ur l'imprimante. Ce champ n'est pas obligatoire. (Ex. : Imprimante de réseau HP 2200) ;
3. `Localisation` d'une imprimante dans l'entreprise. Ce champ n'est pas obligatoire. (Ex. : Sala 1) ;
4. `Interface` utilisé par l'imprimante pour communiquer. À la disposition, il y a quatre options :
   – port parallèle ;
   – port série ;
   – port usb ;
   – l'imprimante de réseau.
5. `Dispositif` que l'imprimante utilise. Elle est directement liée avec l'interface. (Cette option est seulement disponible pour les interfaces port parallèle, port série et port usb) (Ex. Interface -¿ Port Parallèle, Dispositif - ¿ Port parallèle 1)

   Dans le cas d'Imprimantes en Réseau, il faut insérer les champs suivants :
   – `Adresse` d'une imprimante de réseau. (Cette option est seulement disponible pour les imprimantes de réseau) (Ex. : `192.168.1.1`) ;
   – `Port` que l'imprimante de réseau utilise. Ce champ n'est pas obligatoire. (Cette option est seulement disponible pour les imprimantes de réseau) (Ex. comme le cas d'une imprimante HP : 9100) ;

Après insérer une imprimante, pour terminer votre configuretion, il faut que les divers correspondants soient disponibilisés par l'*IPBrick* pour les stations client. Pour faire ça, il faut faire la transfèrement des drivers respectifs de l'imprimante pour le serveur :

1. Faire *netlogon* dans une poste windows comme un utilisateur du groupe d'`Administrateurs` (la station de travail devra être registré dans le domaine de l'*IPBrick*) ;
2. Appuyez sur les touches [Win]+[R] et sur la fenêtre visualisée écrivez `\\ipbrick` ;
3. Sélectionner `Printers et Faxes`
   Vérifier que l'imprimante ajoutée dans l'interface WEB de l'*IPBrick* est présentée.
4. Cliquer le bouton droite de la souris dans la fenêtre de "Printers et faxes" et sélectionner l'option "Propriétés du Serveur" ;
5. Dans la fenêtre présentée, sélectionner l'option "Contrôlables" ;
6. Choisissez "Ajouter", définissez le fabricant et le modèle de l'imprimante et cliquez sur Suivant ;

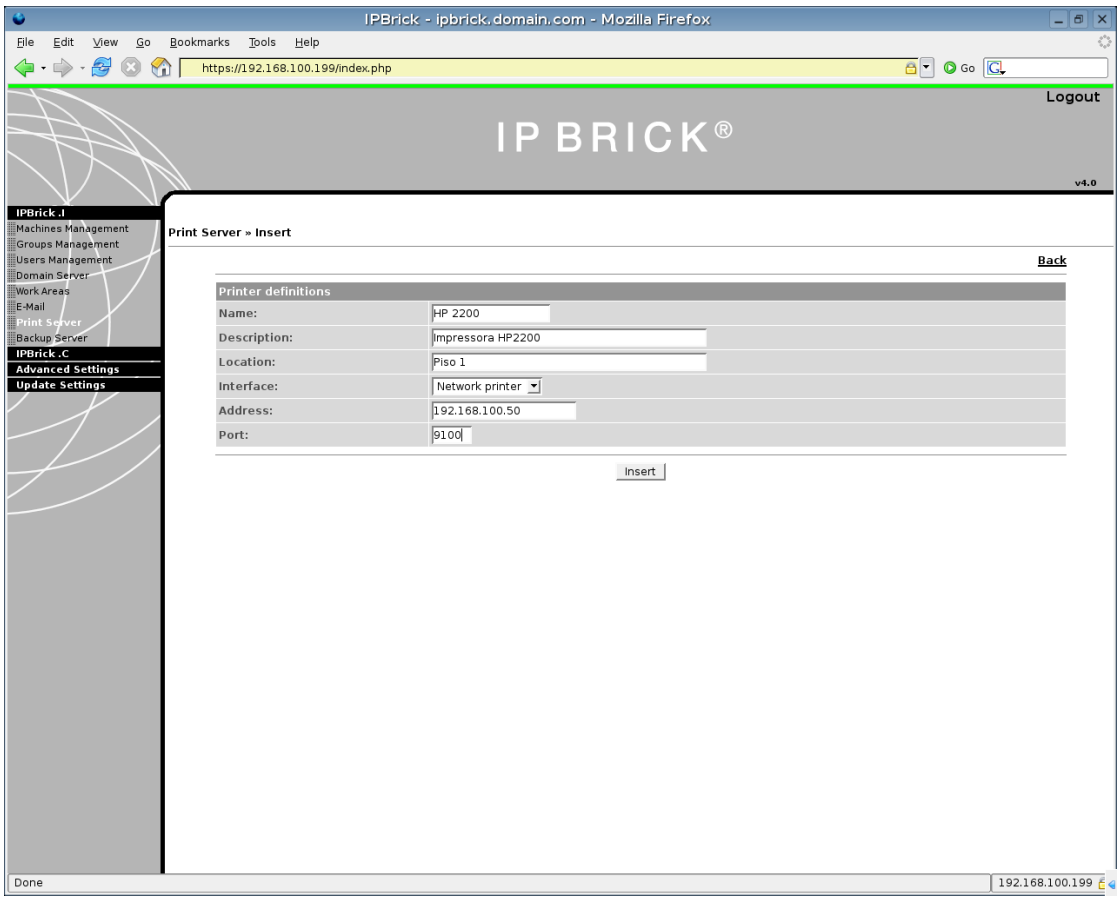

FIG. 3.26 – Insérer une imprimante de réseau

7. Sélectionner les versions du Windows auxquelles les drivers devront correspondre ;
8. Faire `Conclure`.
   Dans ce moment, les *drivers* de l'imprimante sont transférés par l'*IPBrick* ;
9. A nouveau sur le *share* `Printers and Faxes` de l'IPBrick, cliquez-droit sur l'imprimante et sélectionnez les `Propriétés de l'imprimante`. La fenêtre indiquée sur l'Image FIG.3.27[4] apparaîtra et vous devrez choisir "Non".
10. Répondre Non. Entrer en Avancées, sélectionner le driver qui a été ajouté et faire appliquer.

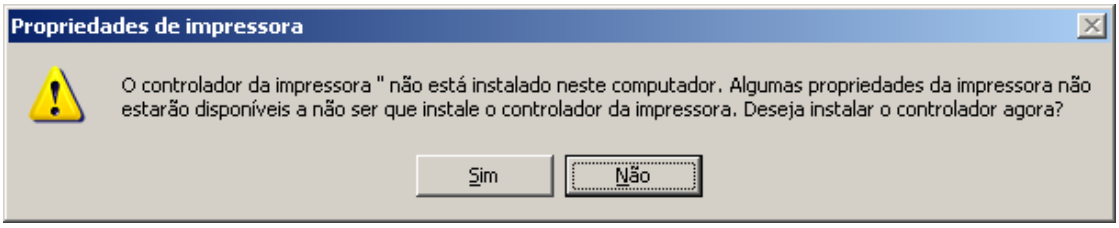
Propriedades de impressora
O controlador da impressora " não está instalado neste computador. Algumas propriedades da impressora não estarão disponíveis a não ser que instale o controlador da impressora. Deseja instalar o controlador agora?
Sim
Não

FIG. 3.27 – Insérer une imprimante en réseau

Pour configurer l'imprimante sur le client, vous devrez :
– Appuyer simultanément sur les touches [Win]+[R] ;
– Ecrire `\\ipbrick` sur la fenêtre créée ;
– Cliquer-droit sur l'imprimante á ajouter et choisir "Brancher".
Vous pourrez vérifier sur les "Imprimantes et Faxes" du client qu'à partir de ce moment l'imprimante est déjà disponible.

3.8 Serveur Sauvegarde

L'option Serveur Sauvegarde permet accéder à l'interface de conFiguretion du Arkeia qui est un software pour la gestion de backups et qui par défaut est installé dans l'*IPBrick*.

En sélectionnant cette option, et après avoir cliqué le bouton `Ouvrir`, une fenêtre de session s' ouvre à travers VNC . Pour réussir la liaison, il faut avoir le JRE[5] installé.

L' authentification dans cette session est effectuée avec le mot-de-passe actuel de l' administrateur de l' *IPBrick*. Suite à la validation, l' interface de gestion Arkeia est disponible.

Pour commencer la configuretion du *software* Arkeia, il faut soumettre la validation par défaut :

[4]Le contrôleur de l'imprimante n'est pas installé sur cet ordinateur. Certaines propriétés de l'imprimante ne seront disponibles, sauf si vous installez le contrôleur de l?imprimante. Souhaitez-vous installer le contrôleur maintenant ?

[5]Java Runtime Environment installé, qui peut être trouvé en `http://sun.java.com/`.

```
login: root
password: <sans mot de passe>
```

La documentation du Arkeia peut être obtenu en `http://www.arkeia.com/manuals.html`.

FIG. 3.28 – Serveur Sauvegarde

Chapitre 4

IPBrick.C

Ce chapitre décrit les menus de l'*IPBrick.C* utilisés pour gérer les principaux services de communications de connexion d'une entreprise à l'Internet. Le menu de l'*IPBrick.C*, comme le menu de l'*IPBrick.I*, est le menu de congiguretion fonctionnel. L'administrateur de l'*IPBrick* dit ce qu'il veut et le software fait les conFigurations et il maintient la consistence des mêmes. Ce chapitre a les suivantes sections principales :

- Pare-feu ;
- Proxy ;
- VPN ;
- Courrier Électronique ;
- Servidor Web ;
- Webmail ;
- VoIP.

4.1 Firewall

⇒ **Remarque: Le changement d'aucune règle du pare-feu implique que le pare-feu soit activé. Si le pare-feu est arrêté dans les services, le changement d'une de ces règles implique le rebouter un fonctionnement du pare-feu.**

4.1.1 Services Disponibles

Présentation L'*IPBrick* a une série de services installés. Une part est en exécution, l'autre est arrêté. Une part est pour l'intranet, les autres sont aussi disponibles pour l'Internet. Dans l'interface ici on indique à pare-feu les services qu'on a en exécution pour l'Internet, de façon à être disponible pour le monde extérieur.

Ces services sont :s

- Serveur Web ; ;
- Serveur de Courrier Electronique ;
- SSH ;
- FTP.

Corpus Dans la liste (`Pare-feu » Services Disponibles`), l'indication de l'état correspond au pare-feu qui est configuré pour permettre le fonctionnement du service - `Actif` - ou au contraire il est configuré pour bloquer les ports des services - `Inactifs`. (FIG. 4.1). Si vous voulez placez ici un certain service comme `Actif`, il ne commence pas le service. Ni l'`Arrête`. Le seul changement appliqué dans l'`Actualisation de Définitions` est faite seulement dans le service du pare-feu qui est arrêté, reconfiguré et après rebouter. D'une façon simple, il ouvre ou ferme le port d'Internet pour le service (si le service fonctionne ou il y a déjà une autre conFiguretion de cette section).

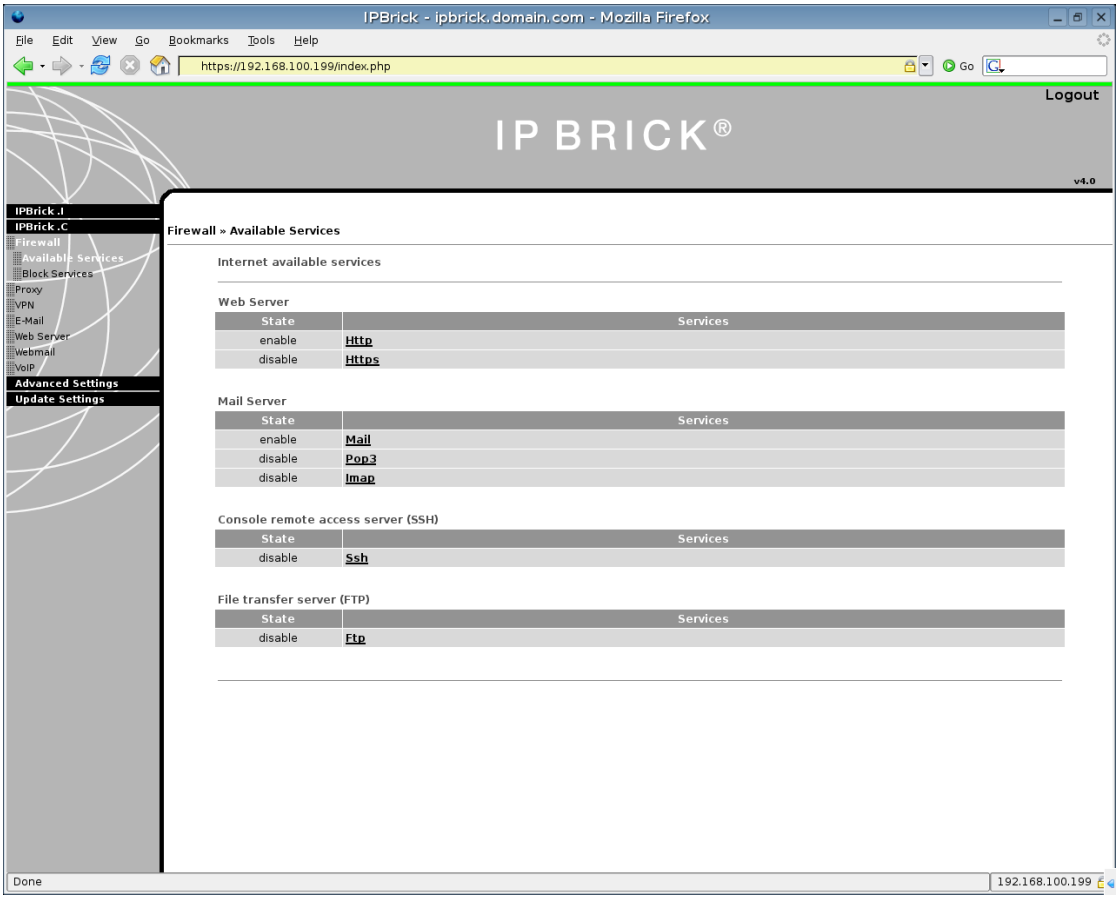

FIG. 4.1 – Pare-feu - Services Disponibles

4.1.2 Bloquer les Services

Présentation L'option de bloquer les services, d'une façon pareille à l'antérieur permet seulement (Pas Bloqué) ou l'êmpeche (Bloqué) le normal fonctionnement des applications indiquées. (FIG. 4.2)

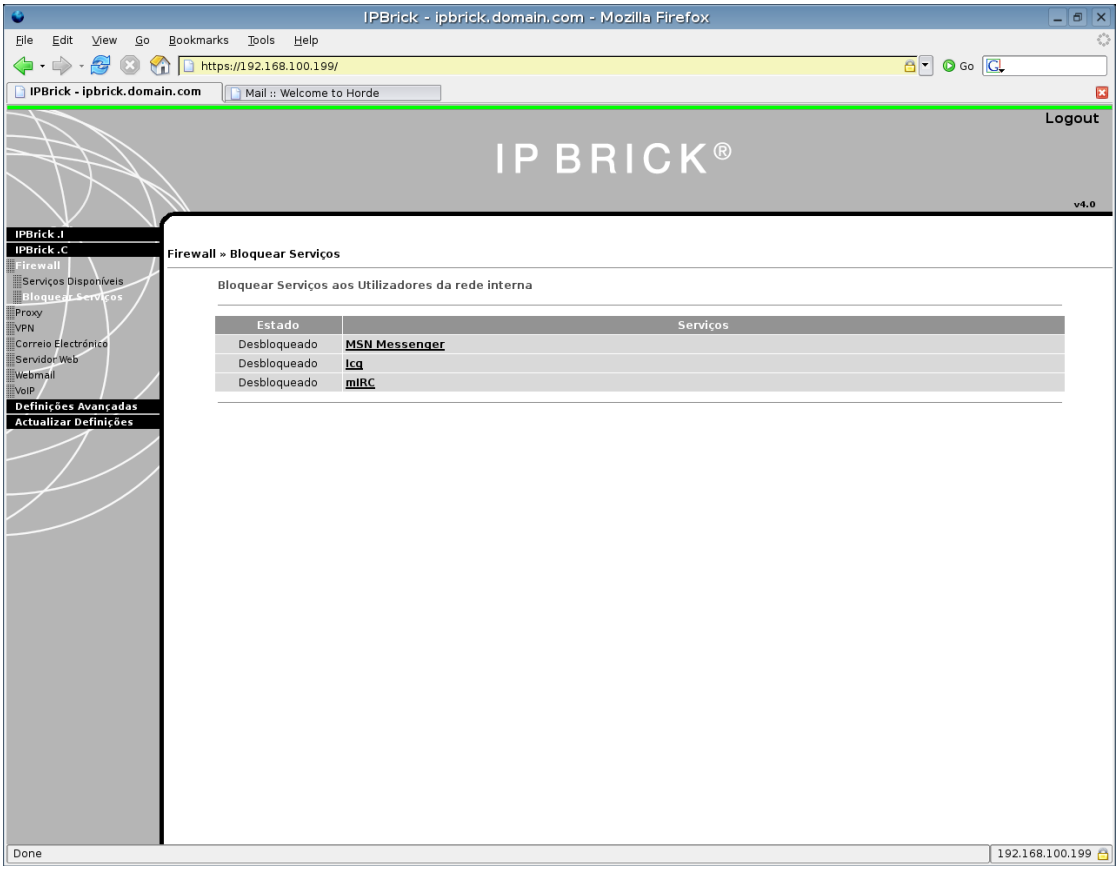

FIG. 4.2 – Pare-feu - Bloquer les Services

4.2 Proxy

Le service de Proxy dans l'*IPBrick* est, quand il est en exécution, à l'écoute des demandes dans le port 3128.

La section est sous-divisée en trois parties, à savoir :

- `Configuretion` ;
- `Statistiques` ;
- `Kaspersky Proxy`.

4.2.1 Configuration

Présentation La configuretion primaire du proxy ici présentée (Fig. 4.3) ira le normal fonctionnement des browsers de l'Internet. Ainsi, il convient définir chaque sort de Proxy :

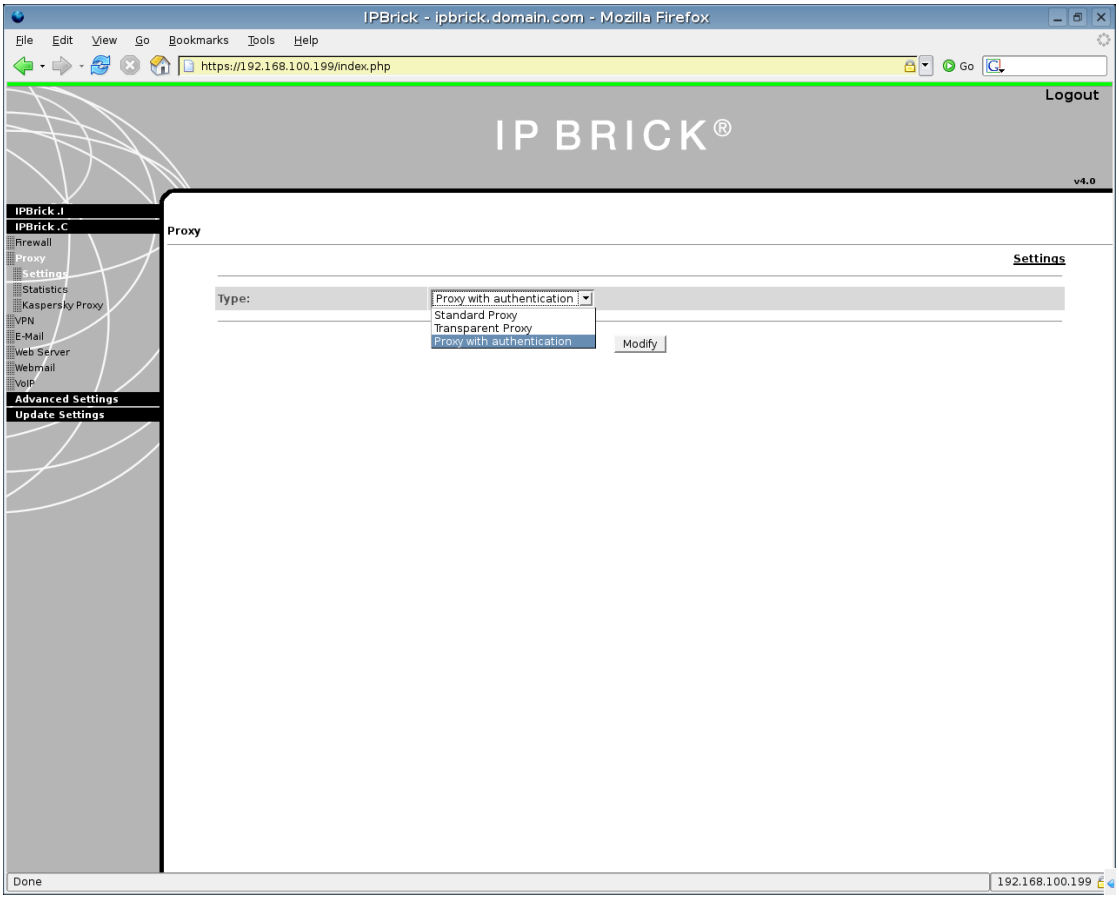

Fig. 4.3 – Proxy - Configuretion

1. `Proxy Étalon` : il n'est pas obligatoire d'utiliser la Proxy pour accéder à l'Internet (Web) et seul utilisera la proxy qui configurer browser pour utiliser la Proxy de l'iPBrick porte 3128. Les utilisateurs sans quelconque conFigure-

tion supplémentaire dans le browser continueront à accéder à l'Internet sans quelconque problème. Pare-feu peut être désamorcé ! ;

2. `Proxy Transparent` : out l'accès à l'Internet (Web) est faite par la Proxy. C'est obligatoire que pare-feu soit actif. Les utilisateurs pourront configurer leurs browsers pour utiliser la proxy indiquée, comme ils pourront aussi continuer à accéder sans configurer quelconque proxy dans son browser. Ici, le pare-feu fait le détour du trafic web pour la proxy. Les accès web sont enregistrés par machine (IPs) à des buts statistiques ;
3. `Proxy avec authentification` : l'accès à l'Internet (Web) est seulement possible en utilisant la Proxy. Les utilisateurs devront configurer son browser pour utiliser la Proxy indiquée, autrement vous n'aurez pas accès au Web. Une fois configurés les browsers, les utilisateurs chaque fois qu'ouvriront browser et essayeront d'accéder au web on sera demandée une authentification valable. L'authentification des utilisateurs est validée par login et mot de passe définis dans la création des mêmes. C'est obligatoire que pare-feu soit dans exécution. Tous les accès Web seront enregistrés par utilisateur pour effets de statistiques.

Menu Dessu Connexion pour interface de définition de Règles de la Proxy. Dans cette interface nous avons des options comme :

- `Liste de réseaux avec le accès au Proxy` : identifier le(s) réseau(x) IP qui a le accès aux services de la Proxy (sans lesquels vous n'aurez pas accès à l'Internet - Web) Ex. : rede `192.168.1.0/24` ; ou, pc `192.168.1.25/32` ;
- `Liste de machines sans accès au Proxy` : le même que l'antérieur, mais si l'antérieur sélectionnait ceux qui pourraient accéder. Cette règle sélectionne ceux qui ne pourront pas accéder ;
- `Liste des sites qui ne sont pas autorisés` : connexion pour `Insérer` URL's de sites qui devront être bloqués à qui utilise cette proxy.. Ex. `www.playboy.com`, `games.yahoo.com` ;
- `Liste de mots non désirés dans l' URL` : des squelettes de mots typiques doivent être insérés ici pour des URLs non désiréés. Ex. : `xxx` ; `sex`. Les exceptions à ces mêmes mots peuvent être aussi insérées, ainsi comme des URLs importantes que sans le souhaiter aient étés englobéés par les règles déjà citées. Ex. : `support.hp.com/driver?uid=qwin3.xxx.exe` ;

Une liste noire est un ensemble d' entités qui, pour une certaine raison, n' ont pas accès à un certain privilège ou service. Dans l'option Liste Noire, il est possible d'activer ou désactiver, l'utilization de ces mêmes listes. Après avoir cliqué sur l'option, sont disponibles les hipotèses suivantes :

- `Liste Noire Active=OUI` : Active l'utilisation d'une liste noire. Les champs suivants sont remplis par défaut, et peuvent être changés :
  - `Url d' Actualisation` : Adresse d' où on peut télécharger le fichier avec la liste de sites à bloquer ;
  - `Page de renvoi` : Si vous essayez d' accéder à une des adresses bloquées , ce champ vous indique vers quelle page vous serez redirigés ;
  - `Listes noires à utiliser` : Les listes noires sont divisées par categories, comme par exemple : sites pornographiques, drogues, jeux online, etc. Dans

ce champ on peut sélectionner les categories que l' on veut activer.

– `Liste Noire Active =NON` : Désactive l'utilization d'une liste noire.

L' option `Proxy Remote` permet d'indiquer une liste de serveurs *proxy* où on peut chercher des informations en *cache*, avant d'accéder au serveur où sont logés les informations. Cela permet un accès plus rapide à l'information.

– `Liste de serveurs proxy remotes` : Permet de définir la liste de *proxys* remotes ;
– `Ne pas utiliser le proxy remote dans les sites suivants` : si vous ne comptez pas d' utiliser le *proxy* remote dans certaisn sites, ceux-là doivent être mentionnés ici.

En `Autre configurations` quand un utilisateur demande un URL qui sera bloqué, la *proxy* répond avec un page modèle en reportant l'erreur arrivé. Ici on a la chance d'indiquer un URL pour lequel l'utilisateur sera arouteent. Comme par exemple, le page de l'entreprise ou le page d'information plus personnalisé que celle de la *proxy*.

Si on utilise un `Proxy authentifié`, il est possible d' empêcher l' accès au *proxy* à certains utilisateurs. Sélectionner `Proxy authentifié` et ensuite indiquer les utilisateurs à bloquer.

4.2.2 Statistiques

Présentation Les statistiques de la proxy reportent plusieurs comptables depuis :

– traffic par heure du jour, par jour du mois ou par mois ;
– Volume de trafic ;
– Sites plus visités ;
– Nombre de visites.

Corpus A la liste présente 3 parties :

– `Statistiques générales` : dans lesquelles est un link pour statistiques de cache et un autre pour statistiques d'accès (Fig. 4.4) ;
– `Statistiques par machine` : où sont acquittées les accès à l'internet de chaque machine (Fig. 4.5) ;
– `Statistiques par utilisateur` : qui présente les statistiques d'accès par utilisateur lesquelles seront seulement mis à jour quand soit sélectionnée l'option `Proxy avec authentification`. (Fig. 4.5) ;

4.2.3 Kaspersky Proxy

Dans cette section il est possible d' activer la licence du Kaspersky pour le *proxy*, de façon à protegér les données qui sont transférées.

4.3 VPN

Présentation

À travers VPN c'est possible d'accéder aux ressources/services de l'intranet

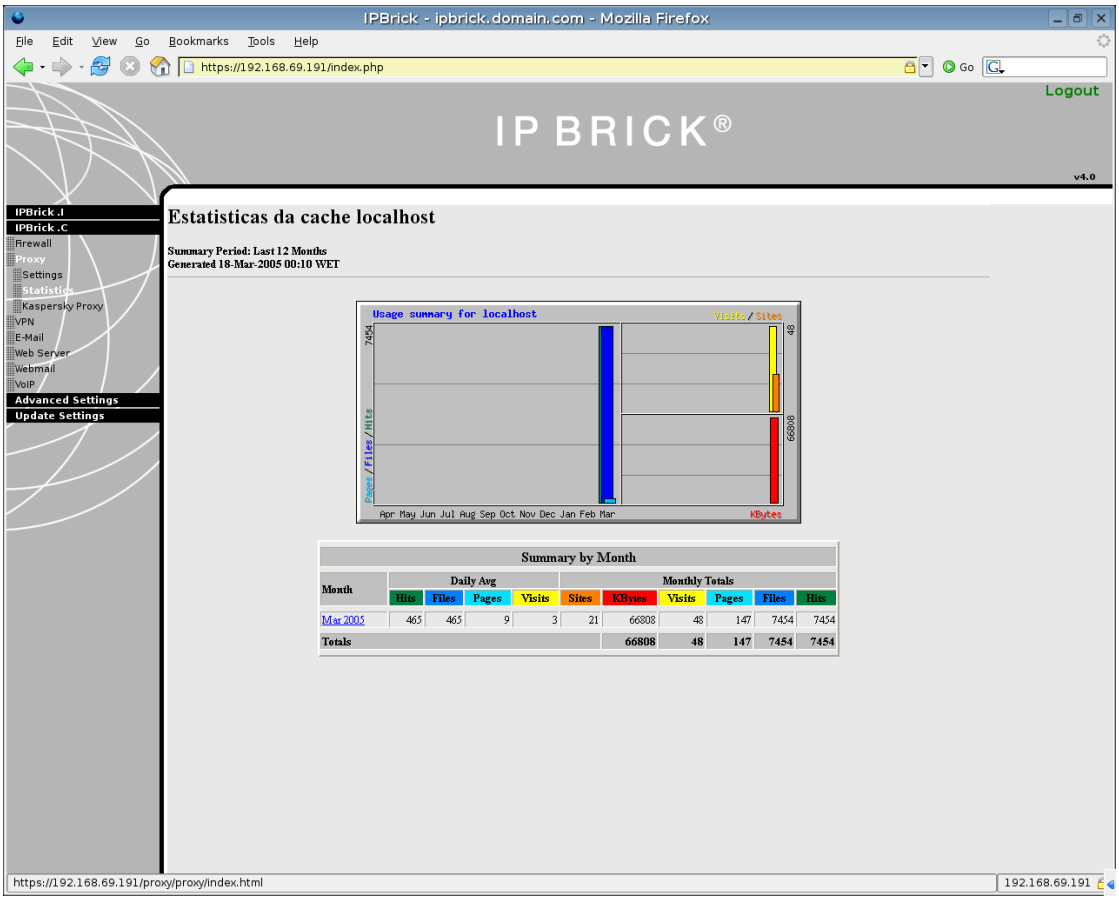

FIG. 4.4 – Proxy - Statistiques de Cache

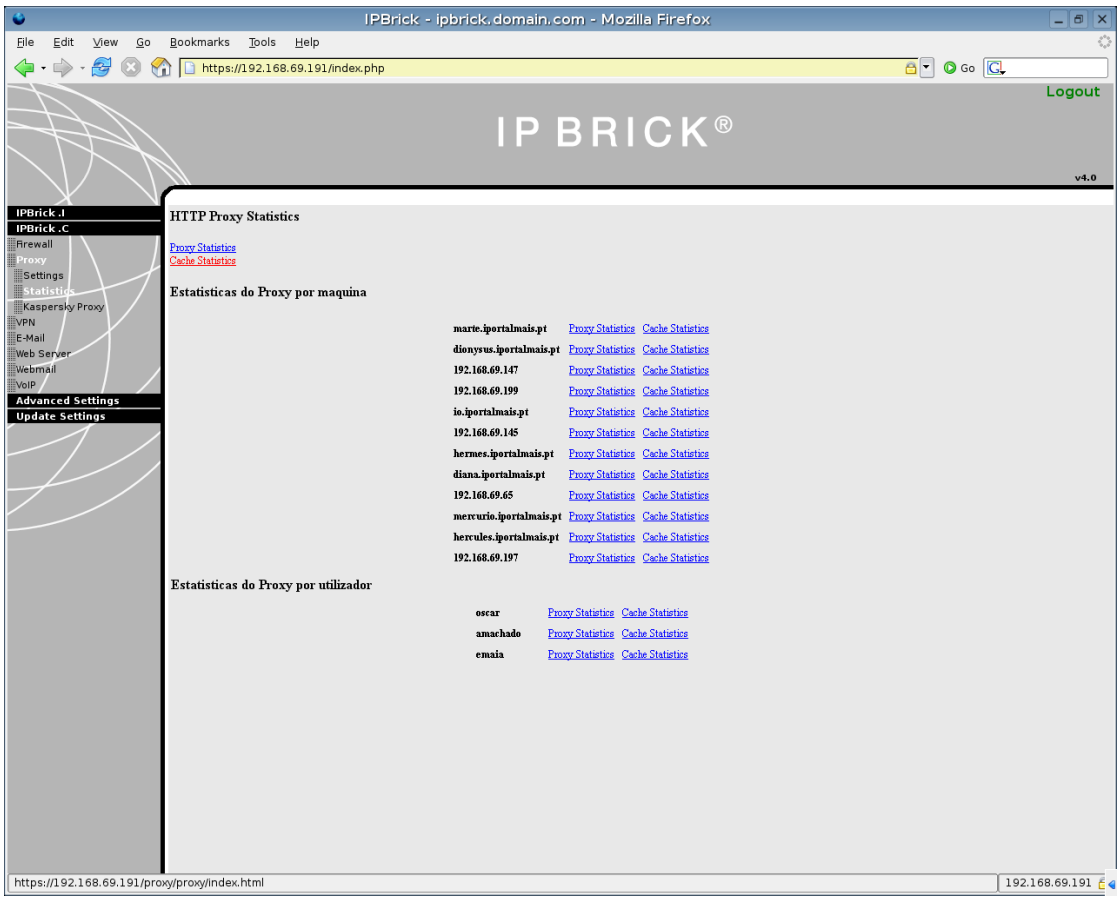

FIG. 4.5 – Proxy - Statistiques par l'utilisateur

d'une entreprise, à partir d'une Connexion éloignée. Cet accès privilégié est restreint à quelques utilisateurs, normalement les nécessaires. Ici nous avons l'interface pour sélectionner les utilisateurs valables.

4.3.1 PPTP

Gestion des utilisateurs

Corpus

Dans la FIG. 4.6, la liste d'utilisateurs du côté gauche correspond aux utilisateurs sélectionnés pour le VPN tandis que du côté droit ils se trouvent les utilisateurs enregistrés dans l'*IPBrick*.

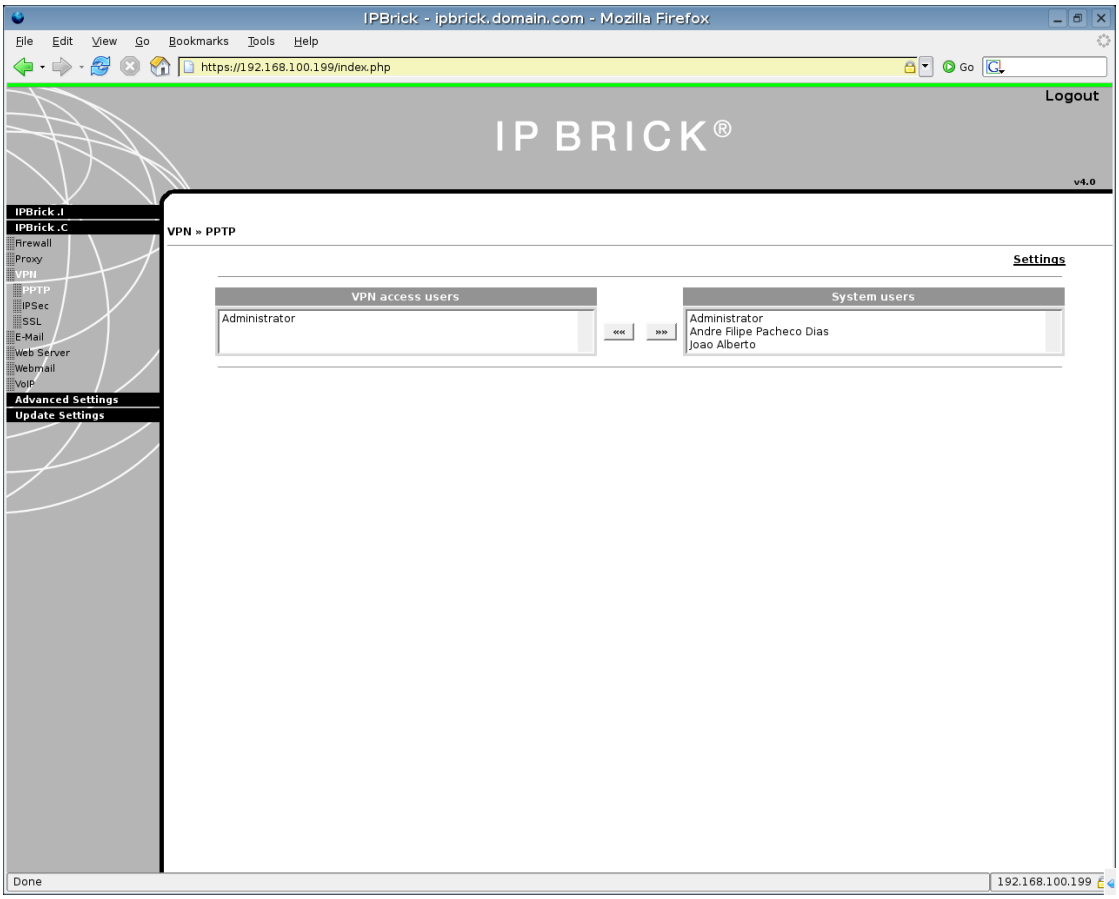

FIG. 4.6 – VPN - Utilisateurs

Menu Dessus

Nous avons une Connexion de Configuretions par laquelle nous accédons à un formulaire où nous pouvons définir le gamma d'adresses IP attribuées (à la disposition) pour les Connexions voit VPN. Les clients éloignés quand ils se lieront ici

recevront un IP à l'intérieur de ce gamma et pour tous les cas sera comme s'ils étaient connectés au réseau dans le serveur avec l'IP dans le gamma ici indiqué.

4.3.2 IPSec

Présentation

L'IPSec[1] est un protocole qui garantit la confidentialité, l'intégrité et l'authenticité des informations transférées à travers de réseaux IP. Au contraire d'un VPN, à travers d'un PPTP ou SSL, le VPN à travers un IPSec permet que deux réseaux (pas deux ordinateurs) puissant communiquer d'une façon sûre.

Corps

En clicant sur `IPSec`, dans le corps de cette section les tunnels IPSec configurés nous sont montrés.

Menu Principal

Il existe une liaison désignée `Insérer`, qui permet d'insérer un nouveau tunnel PSec.

Corps Sur cette page on peut configurer la liaison IPSec (FIG. 4.7). Il faut avoir les données suivantes :

- `Définitions du Réseau Local`
  - `IP Local` : Adresse de l'interface externe de l'*IPBrick* ;
  - `Réseau Local` : L'adresse du réseau local et son masque de réseau ;
  - `Gateway Local` : L'adresse de l'interface interne du routeur du réseau local ;
  - `Identificateur Local` : Adresse de l'interface externe du routeur.
- `Définitions du Réseau "Remote"`
  - `IP Remote` : Adresse de l'interface externe de l' *IPBrick* remote ;
  - `Réseau Remote` : L'adresse du réseau "remote" et son masque réseau ;
  - `Gateway Remote` : L'adresse de l' interface interne du routeur du réseau "remote" ;
  - `Identificateur Remote` : Adresse de l' interface externe du routeur.
- `Gestion des Clés`
  - `Password / mot-de-passe` : Une *Pre-Shared Key* est une clé partagée que le service VPN attend comme première option (avant le username et password). Pour que le serveur VPN permette que les procédures d' authentification continuent, il faut passer la PSK correcte.
  - `Type` : L'IPSec fournit deux modes d'opérations specifiées dans ce champ, le `Tunnel` (où tout le paquet IP original est encripté) et `Transfert` (les données (*payload*) sont encriptées, mais l'entête IP original ne change pas) ;
  - `Authentification` : Aux paquets IP peuvent être additionnés deux nouveaux entêtes, `AH` e `ESP`. En associant le premier à un paquet IP, il garantit l' intégrité et l' authenticité des données, mas pas la confidentialité. Le deuxième fournit confidentialité, intégrité et authenticité de l' information.

[1] IP Security Protocol

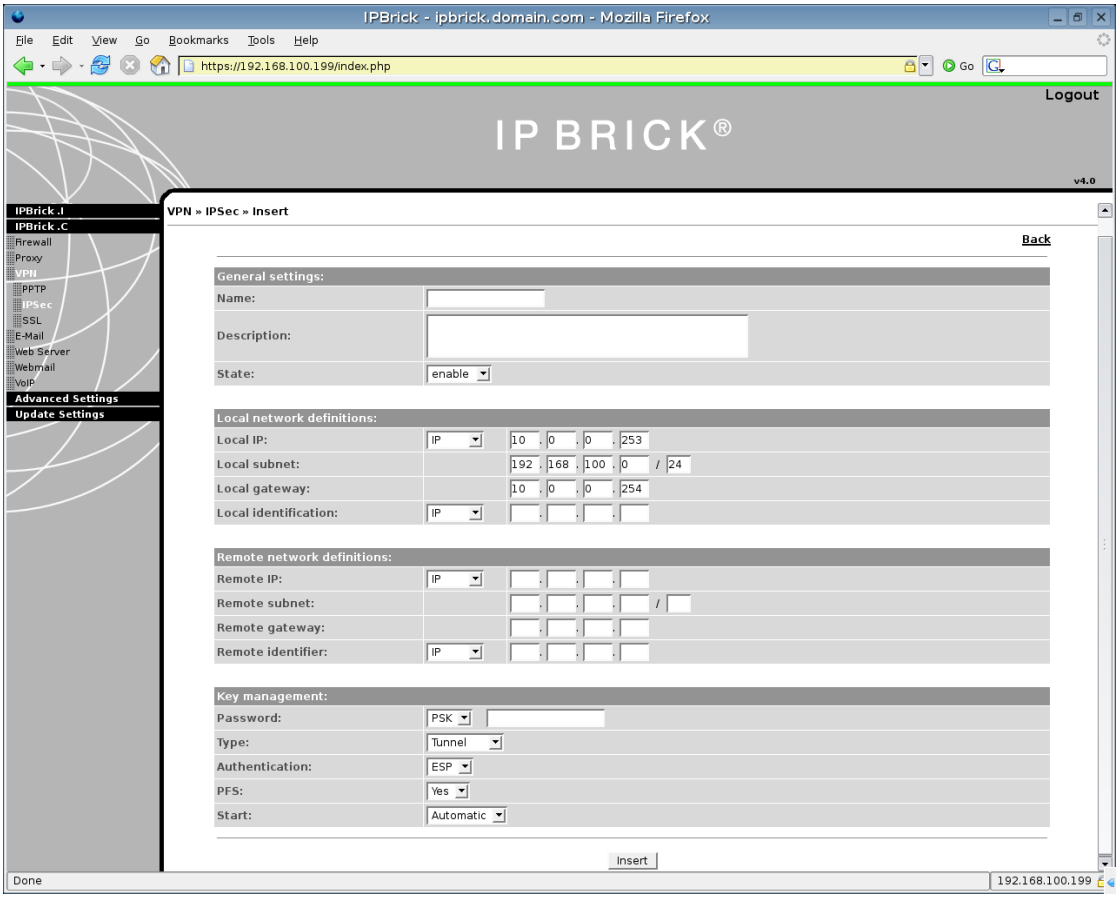

FIG. 4.7 – VPN - IPSec

– `PFS`[2] : Il indique si on veut utiliser le PFS ou non ;
– `Début` : Automátique.

4.3.3 SSL

Présentation

Cette VPN utilise certifié SSL pour établir, légaliser et à encripter les tunnels.

Après avoir cliqué sur `SSL`, le listage des serveurs du VPN SSL apparaît. Pour configurer chacun d'eux, vous devez cliquer sur le serveur souhaité. (Fig. 4.8)

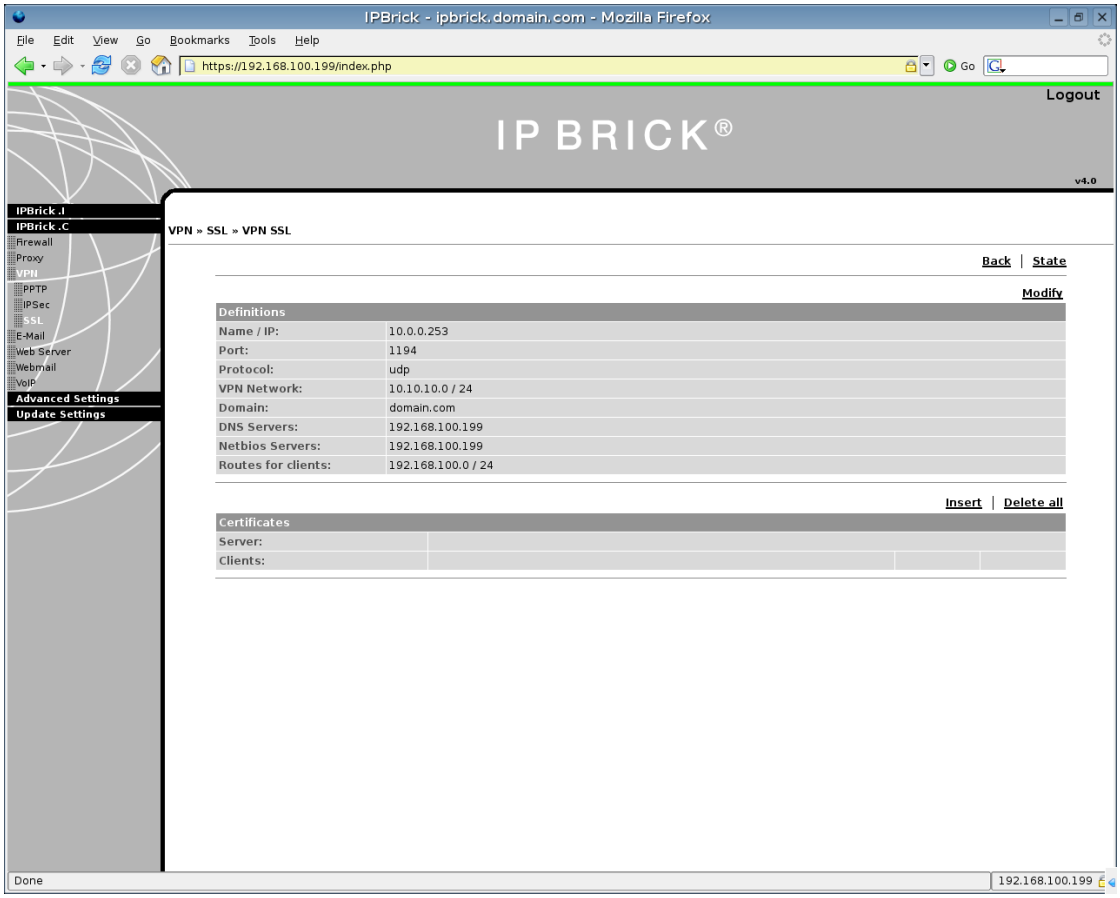

Fig. 4.8 – VPN - SSL

Définitions Dans cette partie, nous pouvons configurer les définitions du réseau du VPN-SSL.

– `Nom / IP` : nom ou adresse IP du serveur ssl ;
– `Porte` : c'est la porte où le serveur du vpn va fonctionner ;
– `Protocole` : c'est le protocole qui va être utilisé pour communiquer ;

[2]Perfect Forward Secrecy

- `Réseau VPN` : c'est le réseau qui va être utilisé pour attribuer un IP aux clients. C'est-à-dire lorsqu'un utilisateur effectuera un vpn pour le serveur, un IP de ce réseau lui sera attribué. Par conséquent, ce réseau ne peut pas exister dans une autre partie du réseau. Dans le cas contraire, cela causerait des problèmes d'acheminement.
- `Domaines` : c'est le domaine qui va être délivré aux clients vpn ;
- `Serveurs DNS` (Système de Noms de Domaine) : c'est le serveur du dns qui va être délivré aux clients vpn ;
- `Serveurs NetBios` : c'est le serveur du wins qui va être délivré aux clients vpn ;
- `Routes pour les clients` : se sont les routes qui vont être délivrées aux clients vpn pour que ceux-ci sachent dans quels cas ils doivent acheminer le trafic par le tunnel.

Certificats

Dans cette partie, on peut créer des certificats qui seront distribués aux utilisateurs vpn. Le premier certificat créé est pour le serveur. Les suivants seront pour les clients. On peut révoquer des certificats en cliquant sur le certificat à révoquer. L'option `Tout effacer` doit être uniquement utilisée pour réinitialiser tout le processus.

Menu Etat

Dans cette interface, on peut voir les tunnels actifs et les trafics respectifs, les utilisateurs et l'IP.

⇒ **Remarque: Après avoir configure ce service, il faut l'activer dans la partie** `Définitions Avancée » Système » Services`**.**

La procédure pour configurer le client vpn est décrite dans l'annexe 9.1.

4.4 Courrier Électronique

La section `Courrier Électronique` se répète dans les deux sources de l'*IPBrick*. Dans l'*IPBrick.I* nous avons les services le plus simple et généralistes comme :

- `Configurer` : les domaines que la machine sert et aroutee ;
- `Gestion des rangs` : permet de consulter la liste de messages qui se trouvent au rang du serveur en attendant d' être délivrés ;
- `Adresses Alternatives` : pour customização des utilisateurs ;
- `Arouteer le Courrier` : pour ré arouteer une copie des messages d'un utilisateur pour autre boîte du courrier ;
- `Kaspersky` : Anti-Virus e Anti-SPAM.

Ces fonctionnalités sont ici répétées et augmentent :

- `Chercher courrier dans ISP` ;
- `Copie du courrier`.

Nous présenterons seulement les nouvelles fonctionnalités vu que les autres déjà ont été présentés ci-dessus.

Présentation

Quand dans une organisation les messages ne sont pas livrés dans un serveur interne de l'entreprise, ils sont seulement disponibles voit POP[3] ou IMAP[4], l'*IPBrick* peut être configuré de manière à décharger périodiquement ces messages de l'ISP[5] pour un serveur local. Une fois dans le serveur local, seront associées aux respectifs comptes préalablement configurés. Ainsi, même si on a accès seulement à un serveur de courrier interne, vous pourrez le configurer pour automatiser et centraliser tous les messages de courrier électronique (de l'Internet et des internes) de l'organisation.

Menu Dessus

Connexion pour `Insérer` les serveurs externes auxquels nous prétendons connecter pour décharger mail et le livrer dans le serveur local. (Fig. 4.9)

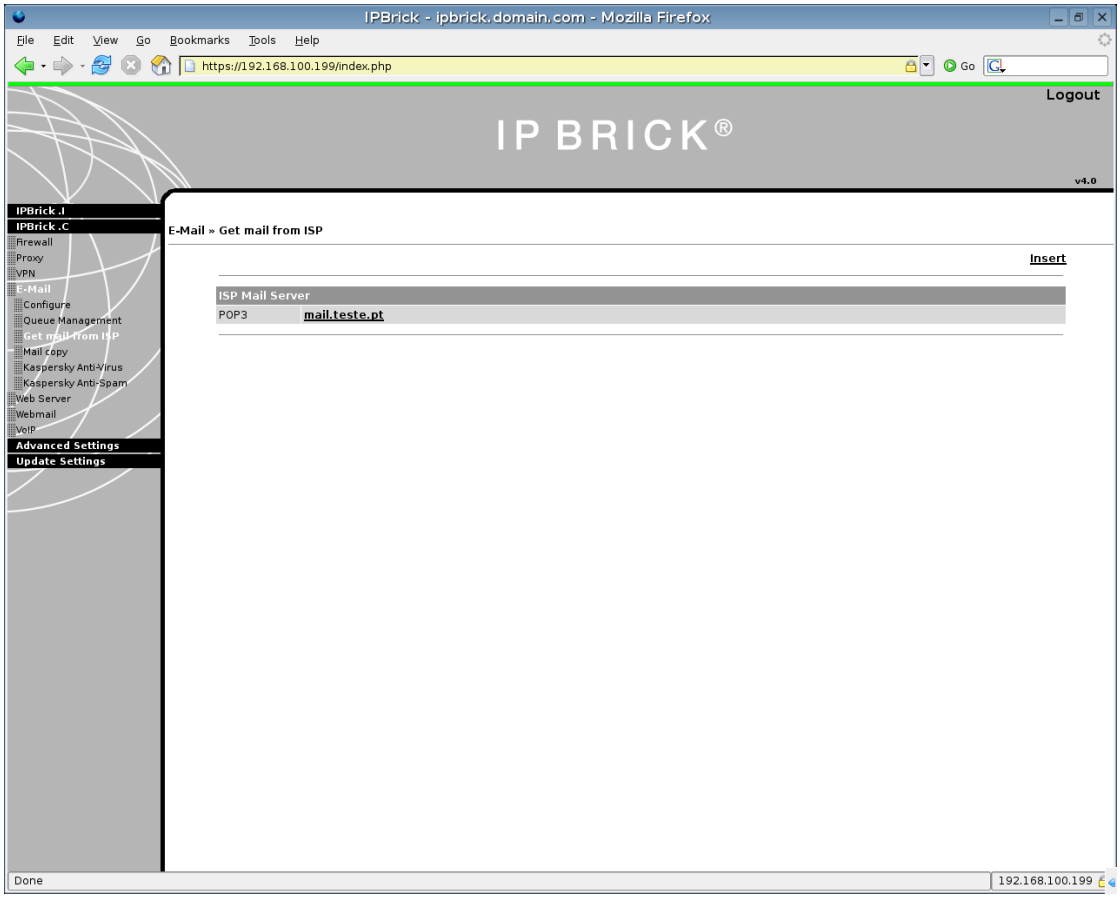

Fig. 4.9 – Chercher Courrier dans l'ISP - Insérer ISP

[3]PostOffice Protocol - c'est un protocole utilisé pour accéder à des boîtes de courrier et de transférer des messages.

[4]Internet Message Access Protocol.

[5]Internet Service Provider

Corpus En cliquant dans un serveur inséré, nous accédons au formulaire de registre du serveur (FIG. 4.10).

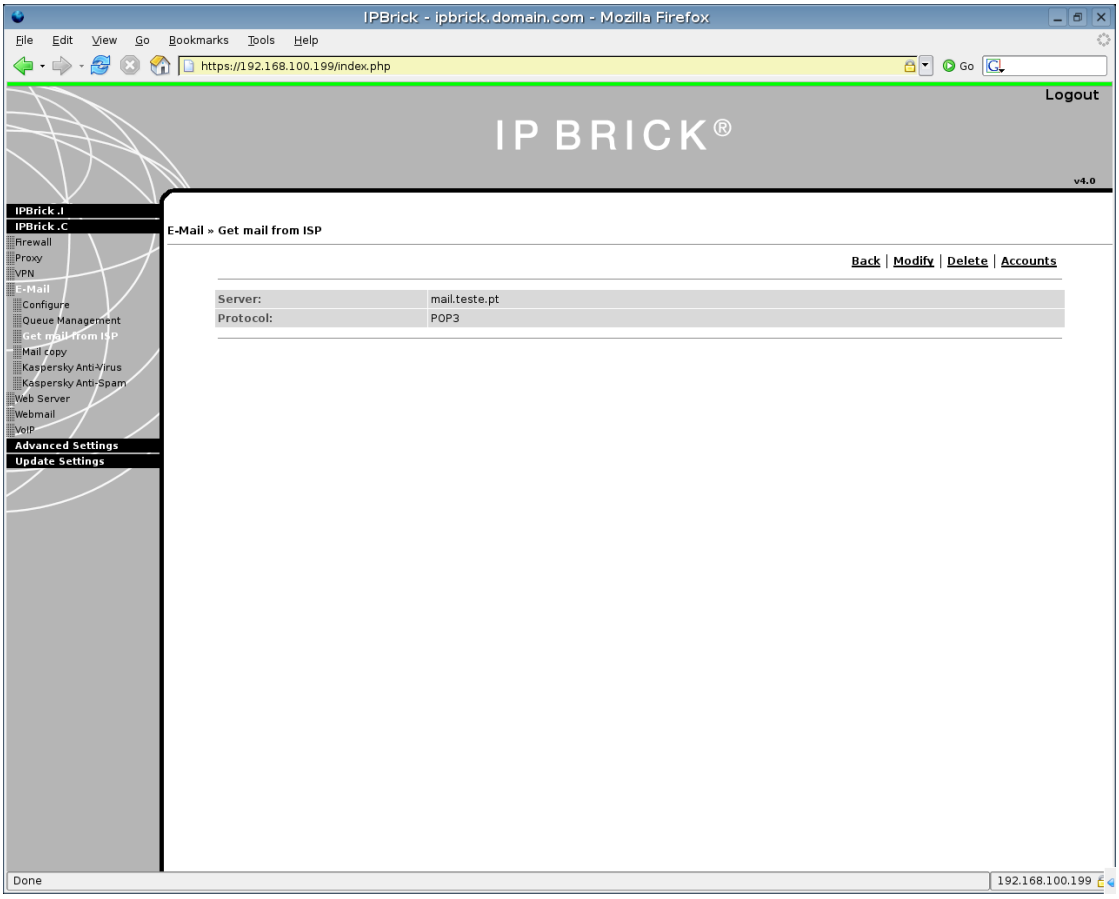

FIG. 4.10 – Chercher Courrier dans l'ISP - Gestion des Serveurs

On peut `changer` ici le serveur et le protocole à travers desquels on accède aux messages, `Effacer` son registre ou passer pour l'interface de gestion des Comptes ou des boîtes de courrier à transférer (FIG. 4.11).

4.4.1 Chercher courrier dans l'ISP

Présentation

Ici nous procéderons au registre des boîtes de courrier poste externes (dans ISP) avec leurs logins et mot de passe. À chacun de ces comptes nous indiquerons le utilisateur local auquel seront livrés mails déchargés.

Menu Dessus

Connexions pour `Rétourner` à la liste des serveurs et pour `Insérer` les comptes qui concerne le serveur sélectionné.
Dans le formulaire d'insertion (FIG. 4.12) vous remplissez les champs :

1. `Login` : pour entrer dans la boîte de courrier éloignée ;

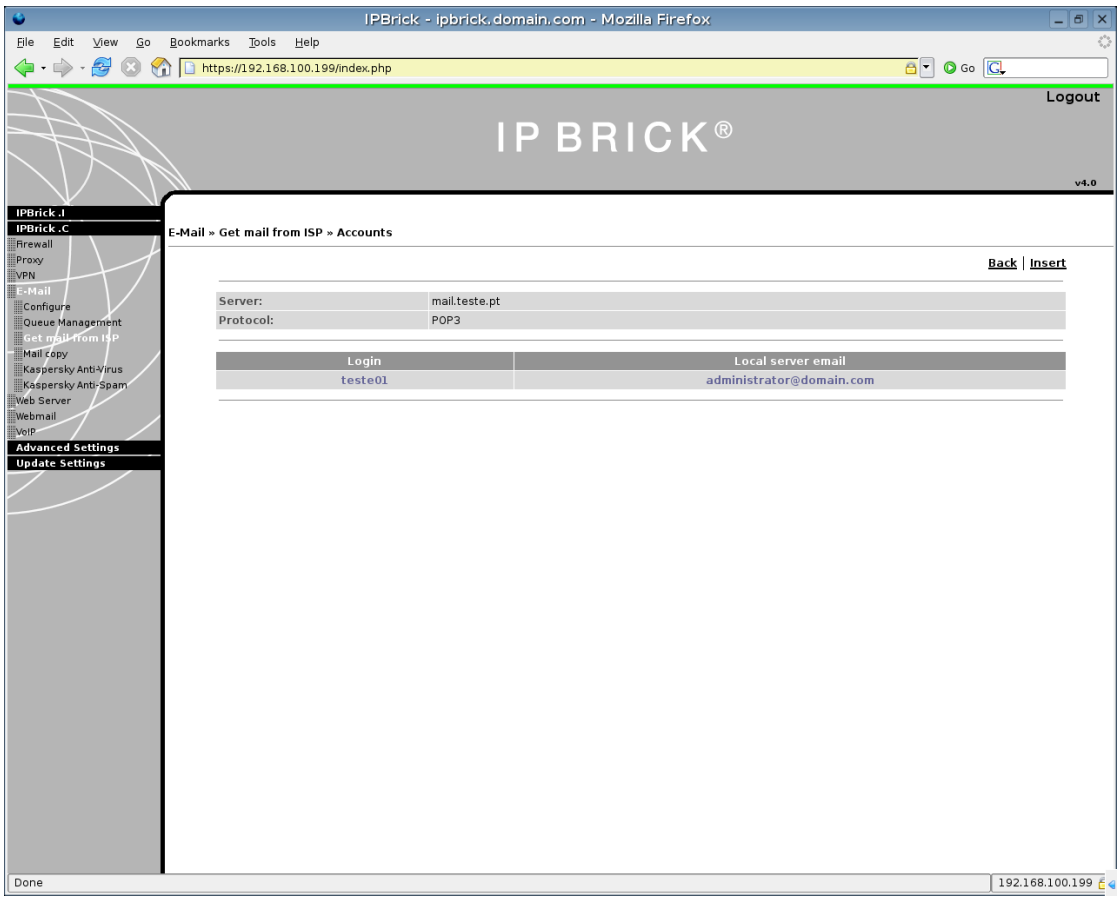

FIG. 4.11 – Chercher Courrier dans l'ISP - Gestion de comptes

2. `Mot de passe` : nécessaire pour valider login ;
3. `Confirmation du mot de passe` ;
4. `Compte local de courrier électronique` : où ils seront livrés les mails déchargés de ce compte ;
5. `Bouton Insérer` et confirmer les données introduites

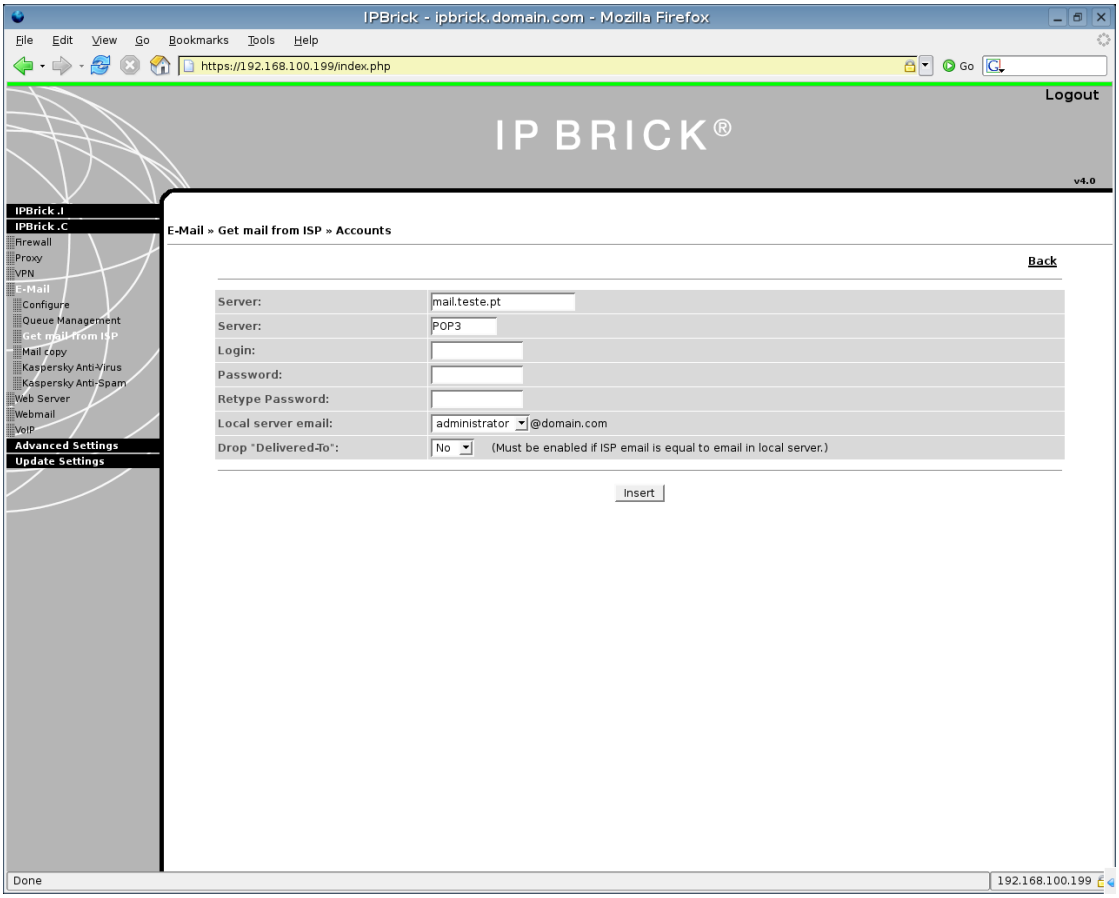

FIG. 4.12 – Chercher courrier dans l'ISP - insertion des comptes

Corpus

La liste des comptes insérés pour le serveur sélectionné permet l'édition des données introduites. Pour ça il suffit cliquer sur la ligne du compte de modifier. Nous sommes arouteés pour un formulaire plus détaillé où nous pouvons maintenant choisir par :

- `Modifier` : les données du compte ;
- `Effacer` : le compte sélectionné ;
- `Tourner` : à vue précédent de la liste des comptes.

4.4.2 Copie du courrier

La Copie de courrier (FIG. 4.13) permet garder toutes les messages de courrier électronique qui entrent et sortent de la société dans deux comptes avec logins reçues et envoyée.

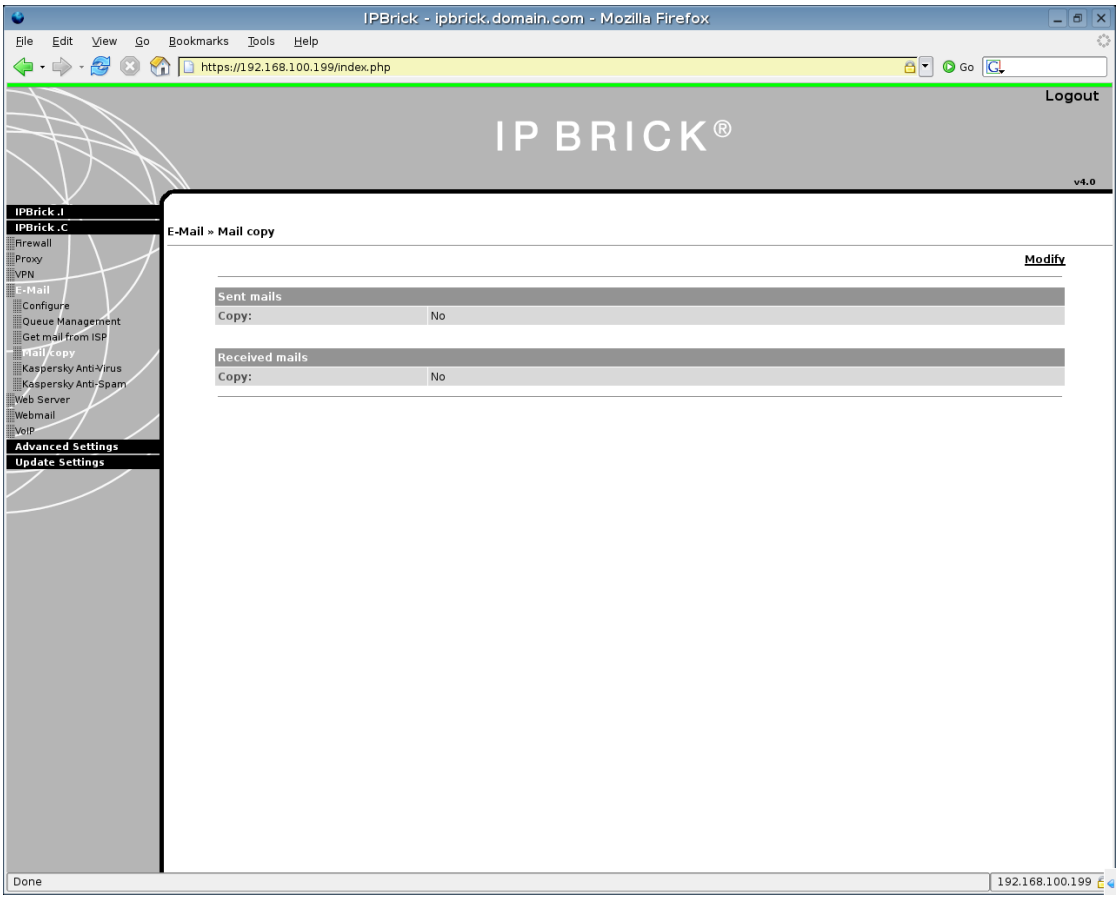

FIG. 4.13 – Copie du courrier

⇒ **Remarque: Il faut être attentif avec la manutention de ces `Copies de courrier`, surtout dans les localisations de beaucoup de trafic de mail. Il est très important maintenir surveillance sur l'évolution de l'occupation de l'espace dans le disque, du serveur, sous peine de ces boîtes de courrier rapidement remplir jusqu'à la totalité de la séparation. À ce moment ils pourront causer quelques bouleversements, soit par interférence avec autres applications du serveur soit par la habitude des responsables par ces boîtes de courrier que à ce moment pourront perdre une série de messages lesquelles on n'a pas été possible d'effectuer copie.**

Présentation

Quand activée (`Oui`) es messages correspondants ils seront copiés pour le res-

pectif compte, c'est-à-dire :

1. `Envoyés=Oui` : toutes les messages qui passent par ce serveur de smtp dont l'expéditeur est quelqu'un du (s) domaine (s) du serveur, seront copiés pour le compte local `envoyé` ;
2. `Reçues=Oui` : toutes les messages qui passent par ce serveur de smtp dont l'expéditeur n'est pas du (s) domaine (s) du serveur, seront copiés pour le compte local `Reçues`.

Quand est activée l'option (`Oui`), le système commence à montrer le champ `Effacer automatiquement les copies:` qui permet définir si les copies de emails existantes dans le serveur sont ou non éteintes. Il permet aussi de spécifier le champ `Effacer des copies avec plus de:` à la fin de combien jours les copies de emails sont éliminées du serveur.

Menu Dessus
Connexion pour `Modifier` la configuretion.

Corpus
Configuretion du service.

4.4.3 Kaspersky Anti-Vírus

Le Kaspersky Antivirus pour Linux mail.server, elle est déjà installé et configuré dans l'*IPBrick*. Pour commencer à l'utiliser vous avez besoin d'introduire une licence valable à travers l'interface correspondante et mettre à jour des définitions dans l'*IPBrick*. Par défaut, les notifications des mises à jour des bases de données et de détection de virus sont envoyées pour que `administrator@domain.com` (Fig. 4.14). Vous devrez modifier ce courrier électronique pour un compte valable dans la machine. Pour plus d'informations sur des conFiguretions, vous devrez consultés les manuels dans `www.kaspersky.com`.

4.4.4 Kaspersky Anti-Spam

Pour accéder à l'interface d'administration, vous devrez utiliser login "administrateur" et le mot de passe sera ce d'administration de l'*IPBrick* (par défaut "123456"). L'interface d'administration est l'original du Kaspersky (Fig. 4.15). our des informations sur cette interface, consulte les manuels dans `www.kaspersky.com`.

4.5 Serveur Web

Présentation
Un serveur web, à travers des protocoles HTTP[6] et/ou HTTPS, est responsable de répondre aux demandes des utilisateurs, concernat ses pages web, ainsi

[6]HyperText Transfer Protocol

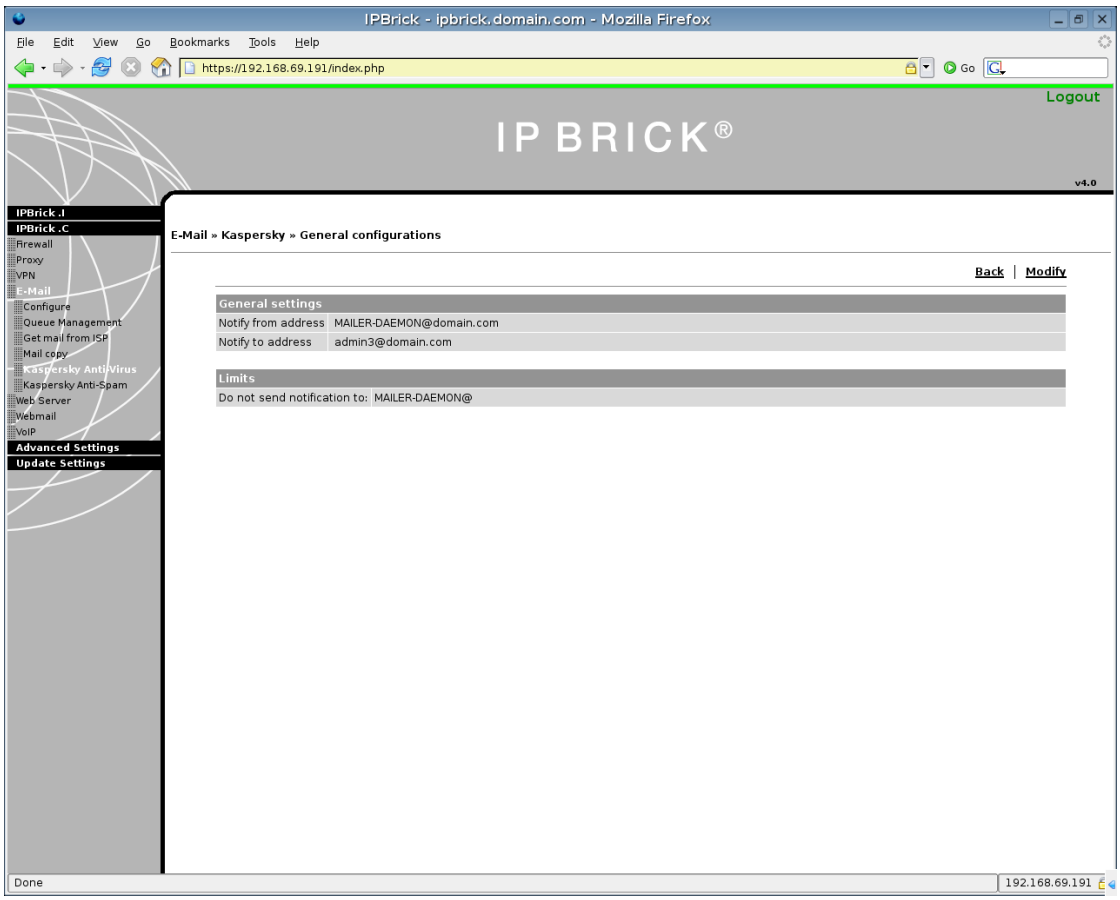

FIG. 4.14 – Kaspersky Anti-Vírus

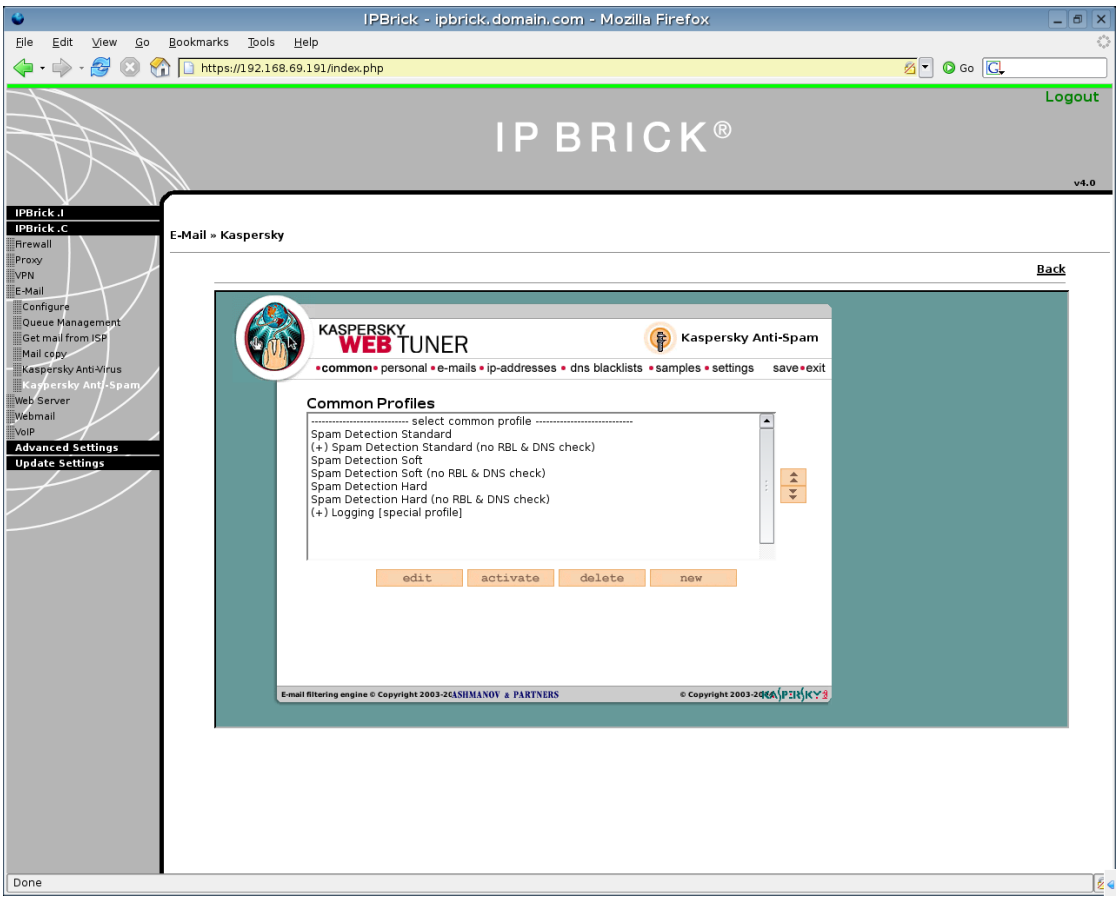

FIG. 4.15 – Kaspersky Anti-Spam

chaque serveur peut loger plusieurs sites. Dans le cas de l'*IPBrick* le serveur web correspondant est le Apache[7]. Les domaines web enregistrés dans l'*IPBrick* sont visualisés après avoir cliqué sur `Serveur Web` et peuvent être vus sur FIG. 4.16.

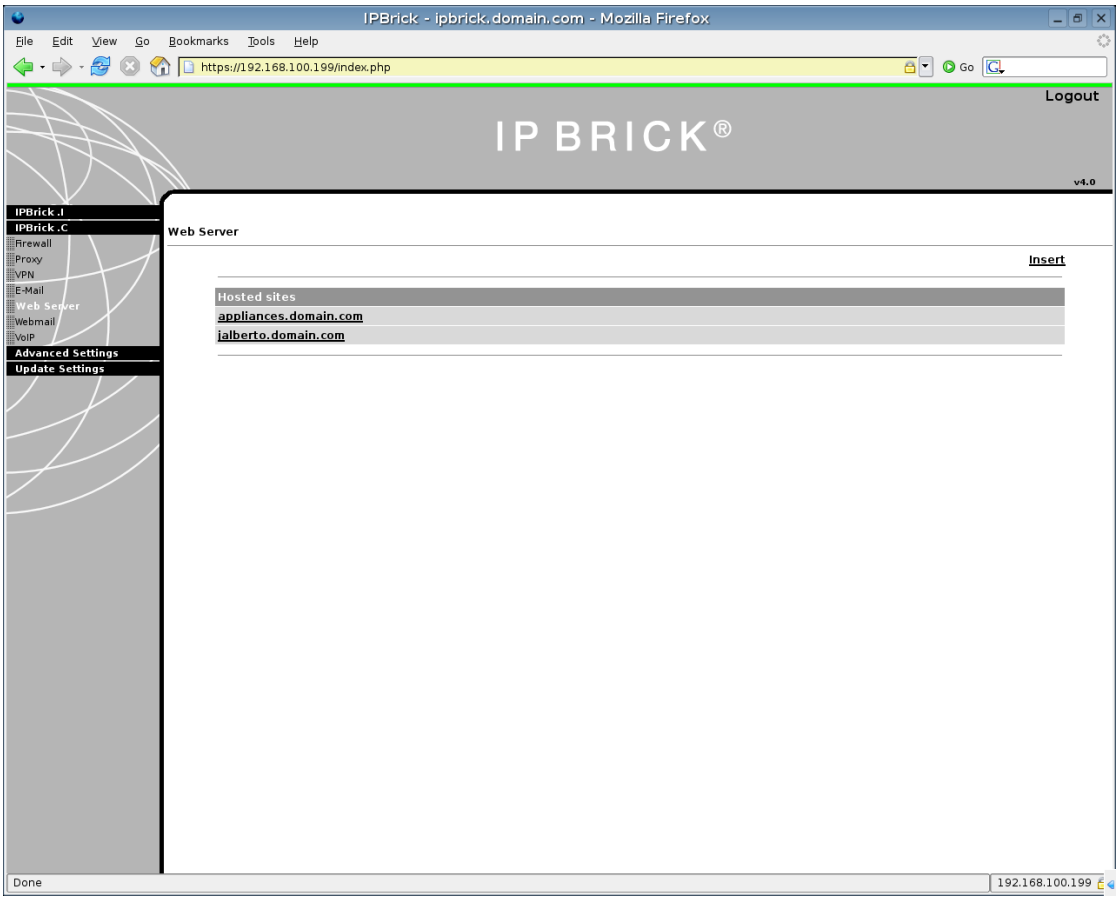

FIG. 4.16 – Serveur Web - Liste des Sites

Menu Dessus

Connexion Pour `Insérer` un nouveau site. Il s'ouvre un nouveau formulaire (FIG. 4.17) où vous remplissez les champs suivants :

1. `Nom` : du site qui se complet avec le selectionné `domaine` selectionné ;
2. `email` : du utilisateur de l'*IPBrick* responsable par la gestion du site.
3. `Utilisateur FTP` : Login de l'utilisateur qui aura accès au répertoire du site à travers de FTP ;
4. `Password` : Password de l' utilisateur précédent ;
5. `Confirmer Password/mot-de-passe` : Confirmation du mot-de-passe.

[7]Renseignements sur urlhttp ://www.apache.org
[7]File Transfer Protocol

6. `Répertoire de localisation du Site` : doit être crée dans le filesystem du serveur. Ce répertoire sera crée en `/home1/_sites/`. Le responsable de ce site a accès a ce répertoire à partir de son compte sur ce serveur.
7. `Disponible pour l'Internet` : indique s'il devra un `VirtualHoust` pour l'IP externe de *IPBrick.C* ;
8. `Bouton Insérer` : et confirmer l'introduction du site.

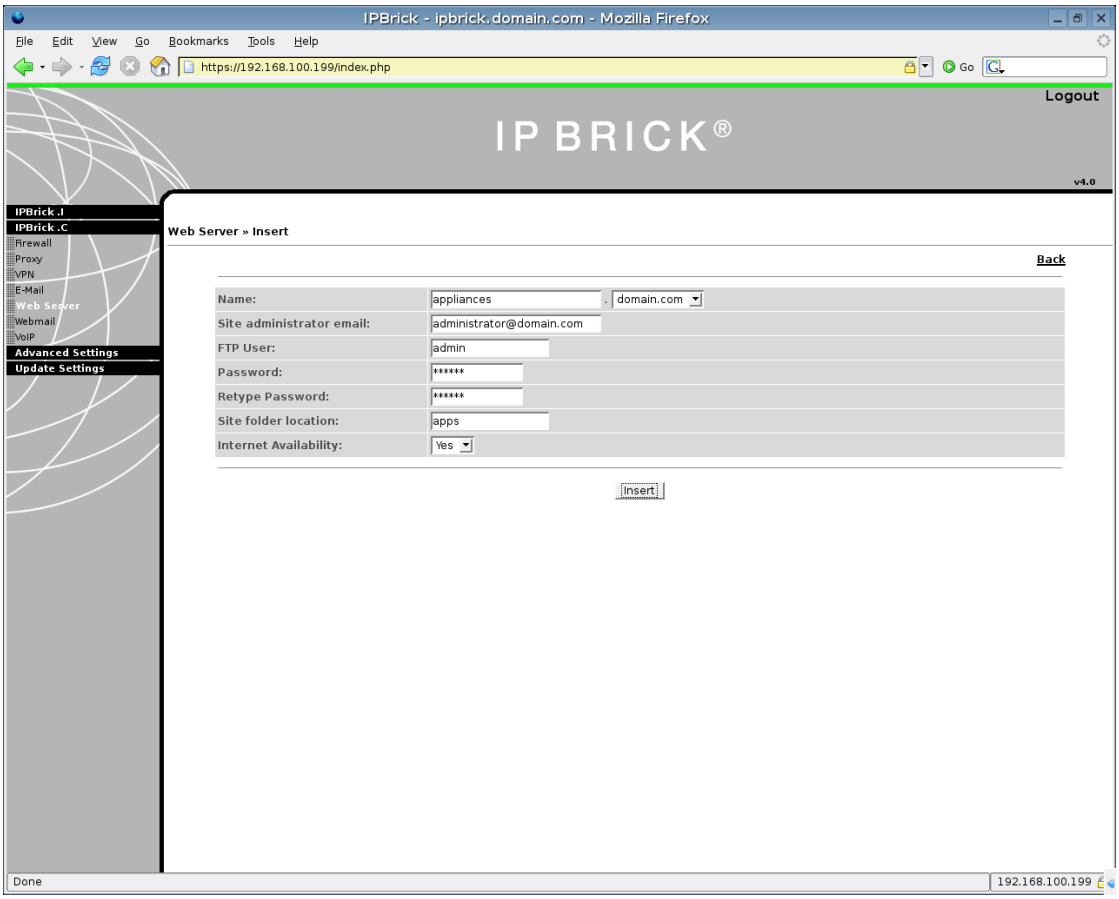

FIG. 4.17 – Serveur Web - Insertion de Sites

Corpus

Liste des sites enregistrés dans *IPBrick*. Chaque ligne est une connexion pour le formulaire de gestion du site. (FIG. 4.18)

Gestion

Présentation

Résumé de l'information du site et les connexions pour la gestion. (FIG. 4.18)

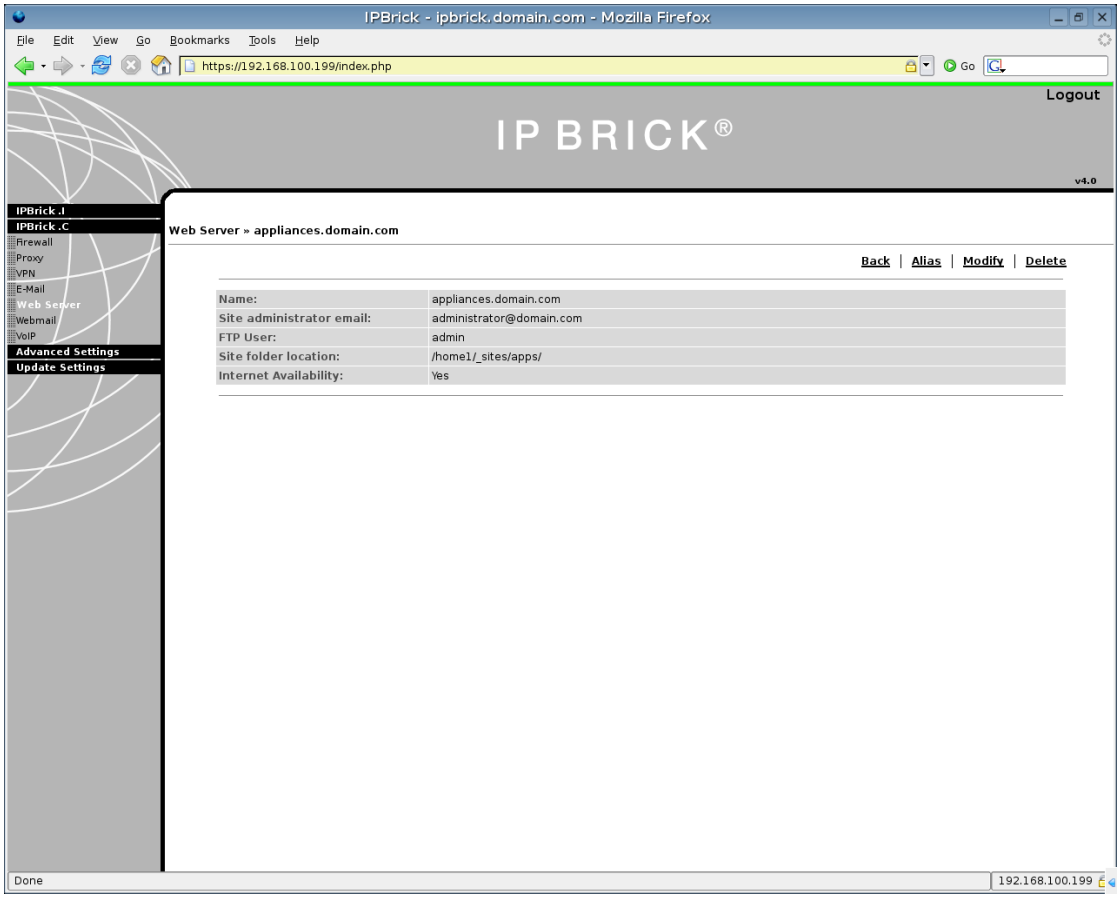

FIG. 4.18 – Serveur Web - Gestion du Site

Menu Dessus

connexions pour :

1. `Changer` : le registre initial du site (responsable, nom du site) ;
2. `Alias`[8] : par ici vous accédez à la liste des registres de ce site et le nouveau page, vous pouvez gérer tous les Alias : (Fig. 4.19) :

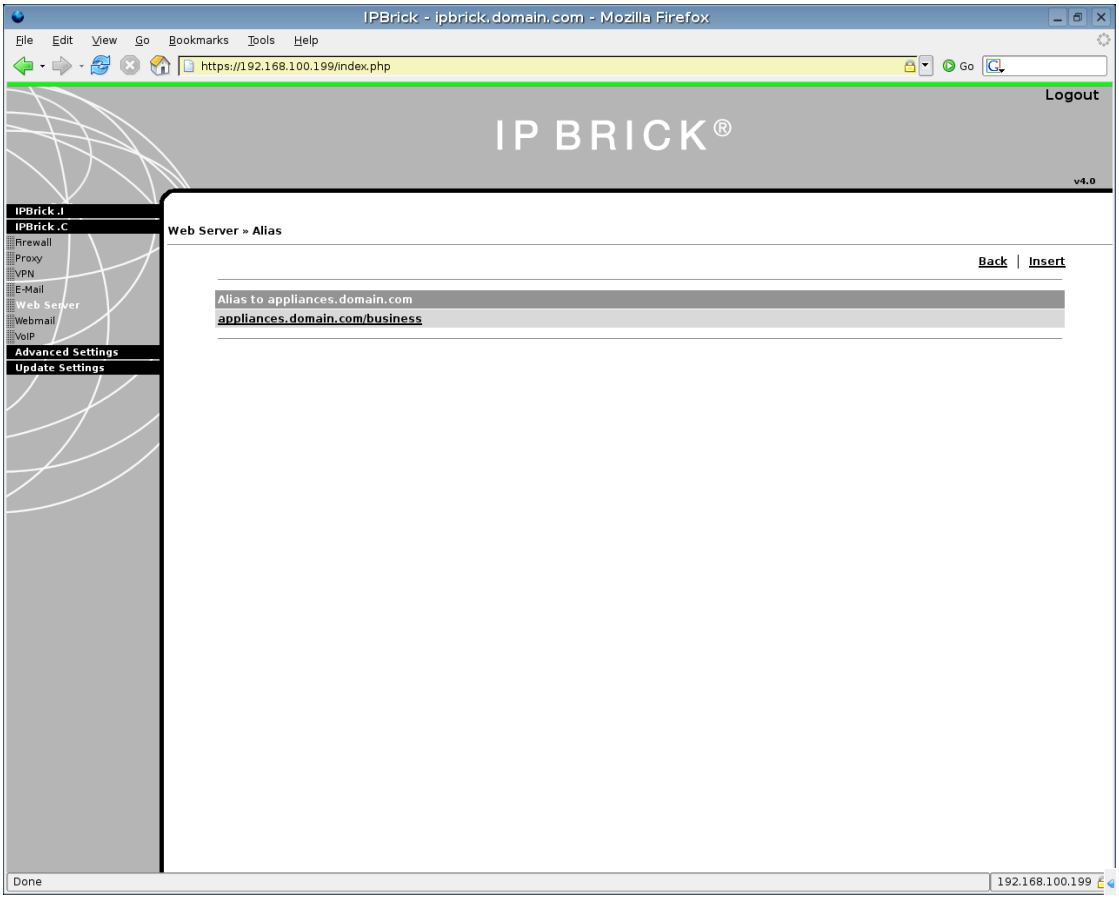

Fig. 4.19 – Serveur Web - Gestion de Alias

- `Insérer` ;
- `Enlever` ;
- `changer` ;
- `Effacer`.

3. `Effacer` :Effacer, enlever le site du serveur Web. Après `Actualiser Définitions` le site ne sera pas disponccherible on-line. Les fichiers du site ne sont pas éliminés, mas ils sont enlevés pour le partage `/home1/sites_bk`[9] accessible

[8] Alias ou HostHeader

[9] C'est la localisation des fichiers des sites enlevés. Tel comme les comptes d'utilisateurs et les partages de groupe, aussi les sites quand enlevés par l'*IPBrick*,on est seulement reconfiguré les services affectés et les contenus sont déplacés pour un partage propre accessible seulement par les administrateurs. Les autres partages de ce type sont Backup1 et Backup2 qui gardent les contenus des secteurs de Travail 1 et 2 respectivement.

par les `administrateurs`. Placé dans le compte, un dossier avec le nom du site écrit. C'est à travers de ce dossier que vous ferez la manutention du site Alias ou HostHeader, simplement une façon d'accéder à certains contenus physiquement déplacés du directory principal du site. Plus informations dans la section d'exemples.

Corpus
Tableau d'information sur le site sélectionné :
- `Nom`;
- `Responsable du serveur`;
- `Utilisateur FTP`;
- `Dossier dans le serveur`;
- `Disponible pour l'Internet`.

4.6 Webmail

Le Web mail installé dans l'*IPBrick* peut être configuré pour gérer les autres serveurs du courrier électronique mais pas l'*IPBrick* où il est installé. Pour ça il suffit indiquer dans cette section les serveurs de IMAP[10] et le SMTP[11] a utiliser.

4.6.1 Serveurs

Présentation
accéder à la boite du courrier électronique (Fig. 4.20)

Menu dessus
Connexion pour `changer` les serveurs installés.

Corpus
Liste des serveurs configurés. Les serveurs pourront être identifiés par son FQDN[12] ou l'adresse IP.

4.7 VoIP

Cette section constitue l'interface de gestion du service VoIP[13] disponible dans *IPBrick*.

[10]Internet Message Access Protocol - accéder à la boite du courrier électronique
[11]Simple Mail Transfer Protocol - envoyer courrier electrónico
[12]Fully Qualified Domain Name
[13]Voice over IP - Service de téléphonie sur l'IP.

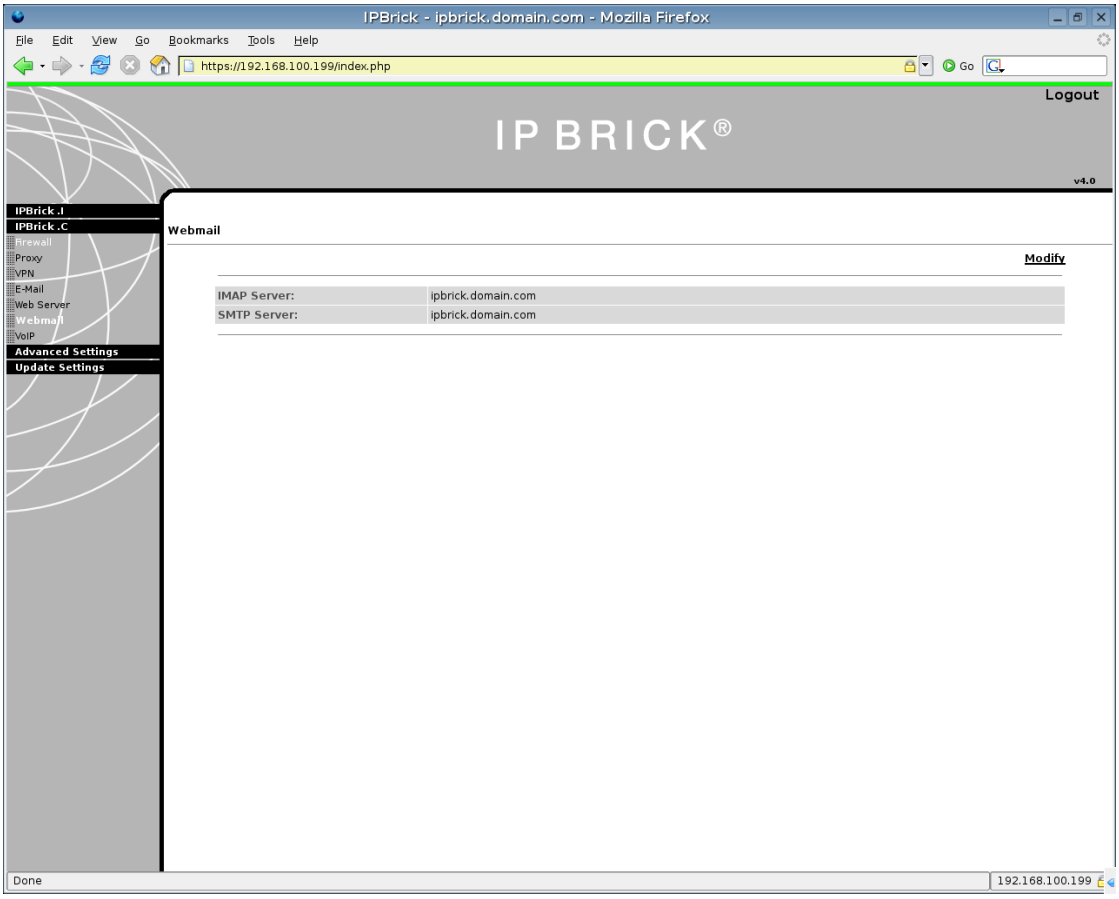

FIG. 4.20 – WebMail - serveurs

4.7.1 Téléphones Enregistrés

Ici (FIG. 4.21), il est possible vérifier les clients VoIP (téléphones IP, station de travail +soft phone) qui sont enregistrés dans *IPBrick*. Le menu pour l'insertion des machines est explicite dans la section 3.1.

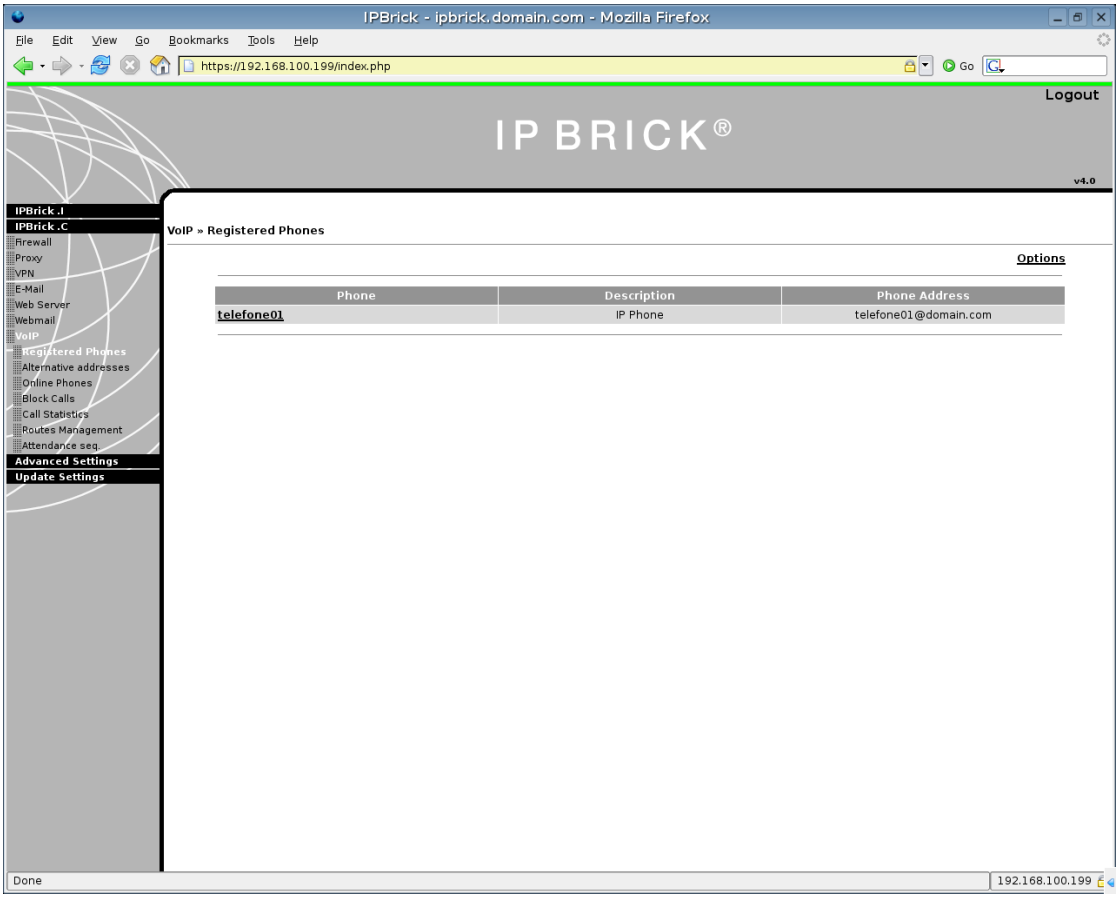

FIG. 4.21 – Téléphones Enregistrés

Dans `Options` on peut configurer les champs suivants (FIG. 4.22) :

- `Routeur avec DNAT total?` : Si l' *IPBrick* est branché à un routeur responsable par l' accès à l' extérieur (en termes de VoIP) qui laisse passer tout le trafic, on doit sélectionner `OUI` et indiquer l' adresse externe de ce même routeur ;
- `Voicemail` : Indique si le voicemail est `Actif` ou `Inactif` ;
- `Timeout de réponse` : Temps qui dure l' appel dirigé au téléphone principal, avant de terminer ou d' être renvoyé vers un autre numéro de téléphone ;
- `Timeout de conexion` : Durée de temps pendant laquelle on essaie d' établir une liaison (secondes) ;
- `Seulement serveur VoIP de l' Intranet` : Serveur de VoIP seulement sur l'Intranet (`Oui`) ou non (`Non`) ;

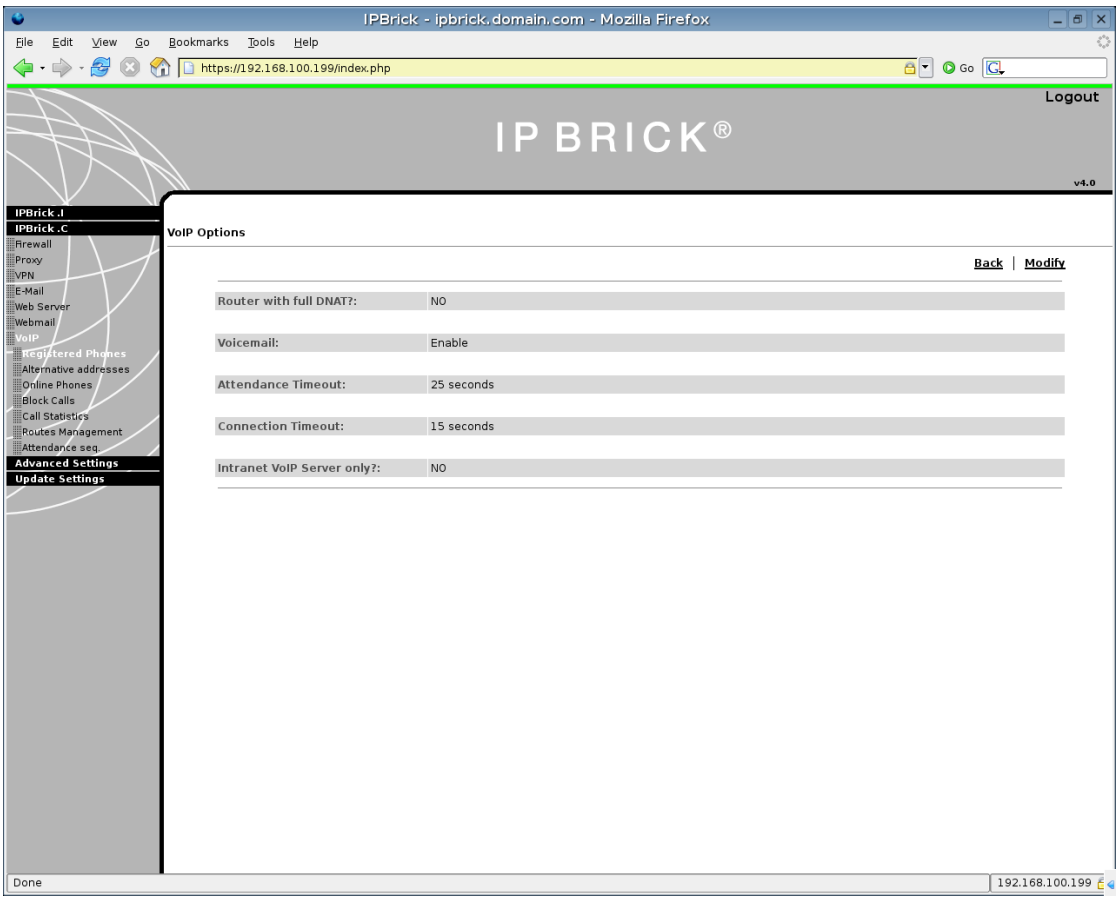

FIG. 4.22 – VoIP - Options

4.7.2 Adresses Alternatives

Dans cet interface (FIG. 4.23) est possible créer adresses alternatives pour les Clients VoIP existants. Par exemple, si le téléphone `5050@domain.com` appartient au cabinet de Jean Henry, vous pouvez créer l'adresse `jeanhenry@domain.com`. Ainsi, le client peut être trouvé par ces deux adresses. Il est possible insérer autres adresses par téléphone/Soft phone.

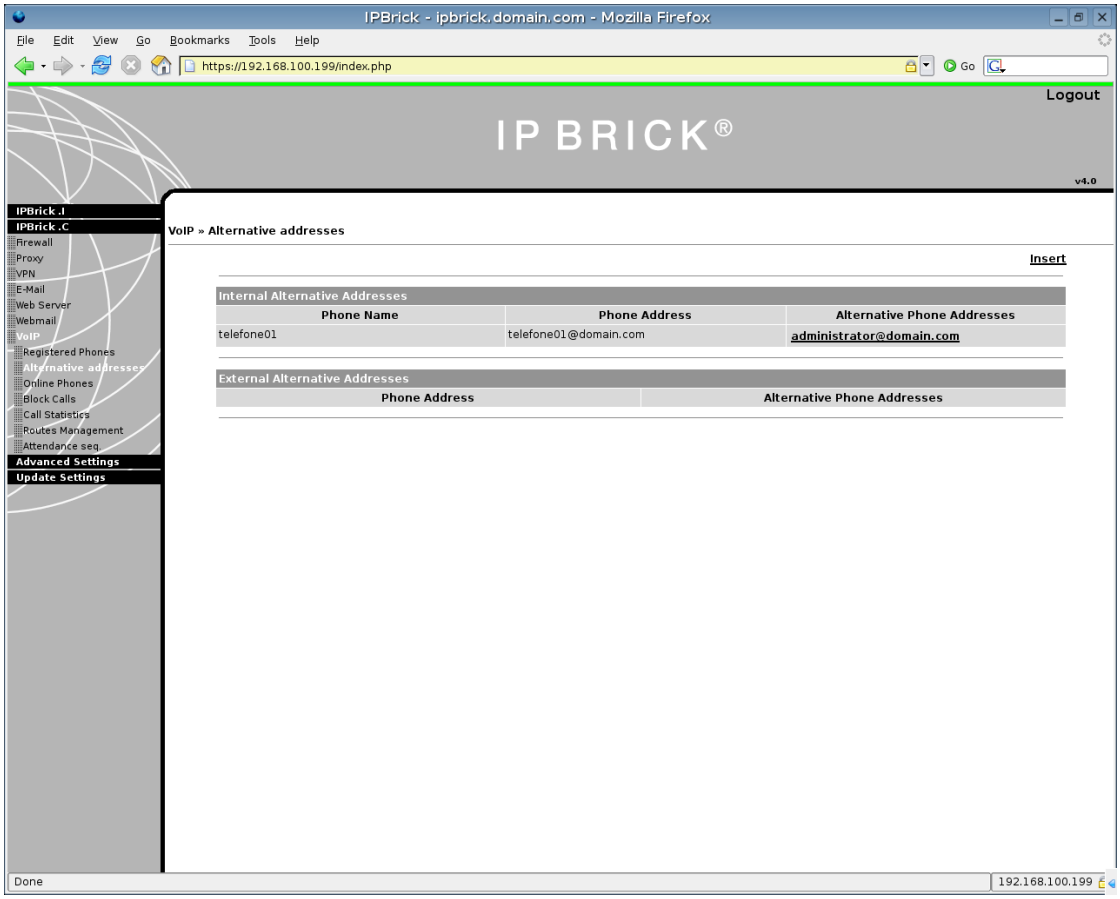

FIG. 4.23 – Adresses Alternatives

4.7.3 Téléphones Actives

Les clients VoIP actuellement on-line sont présentés dans cette interface (FIG. 4.24).

4.7.4 Bloquage d' Appels

Permet de choisir d' entre les `Téléphones enregistrés`, quels sont ceux qui sont authorisés à faire des appels (`Téléphones Authorisés`), comme on peut voir sur FIG. 4.25. Sur `Téléphones enregistrés`, on a la liste des téléphones enregistrés dans l' *IPBrick*. A travers les boutons »» et «« il est possible d' authoriser

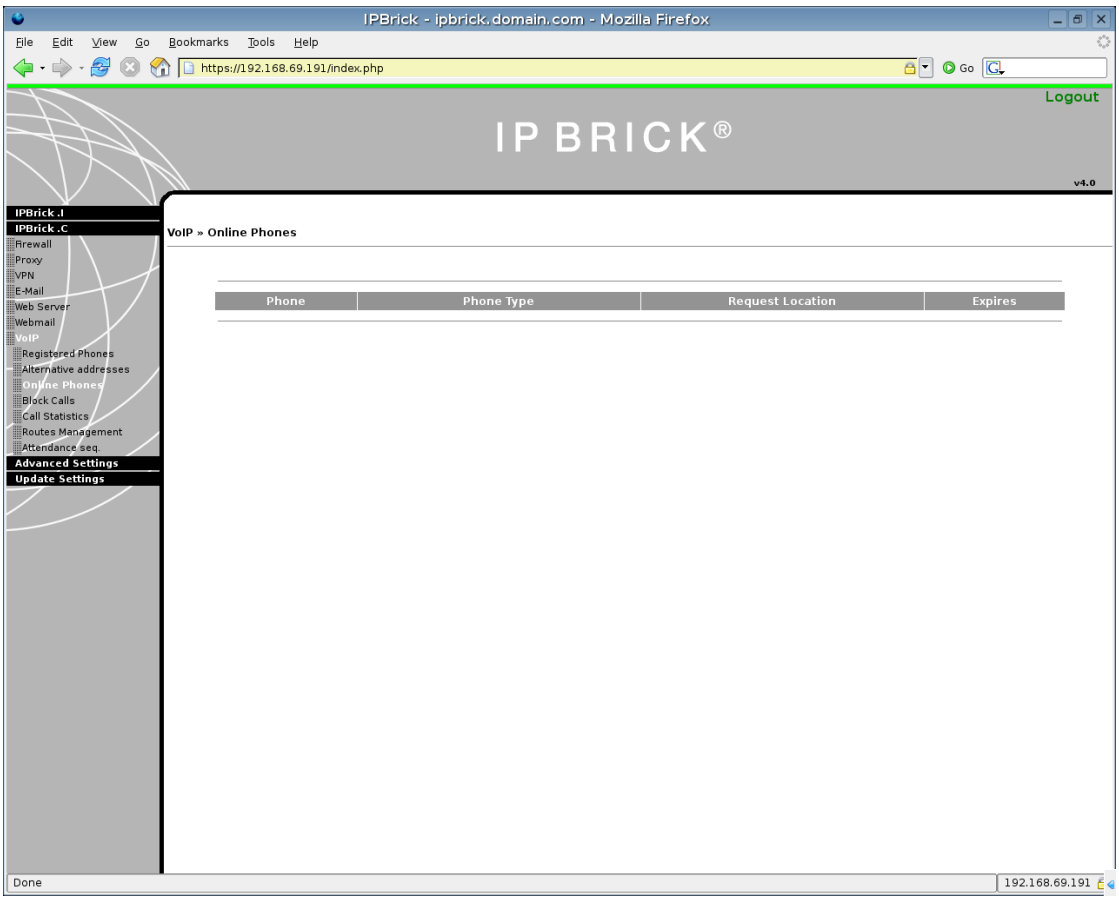

FIG. 4.24 – Téléphones Actives

(passant ainsi à être dans le champ `Téléphones Authorisés`), ou retirer l' accès à un téléphone.

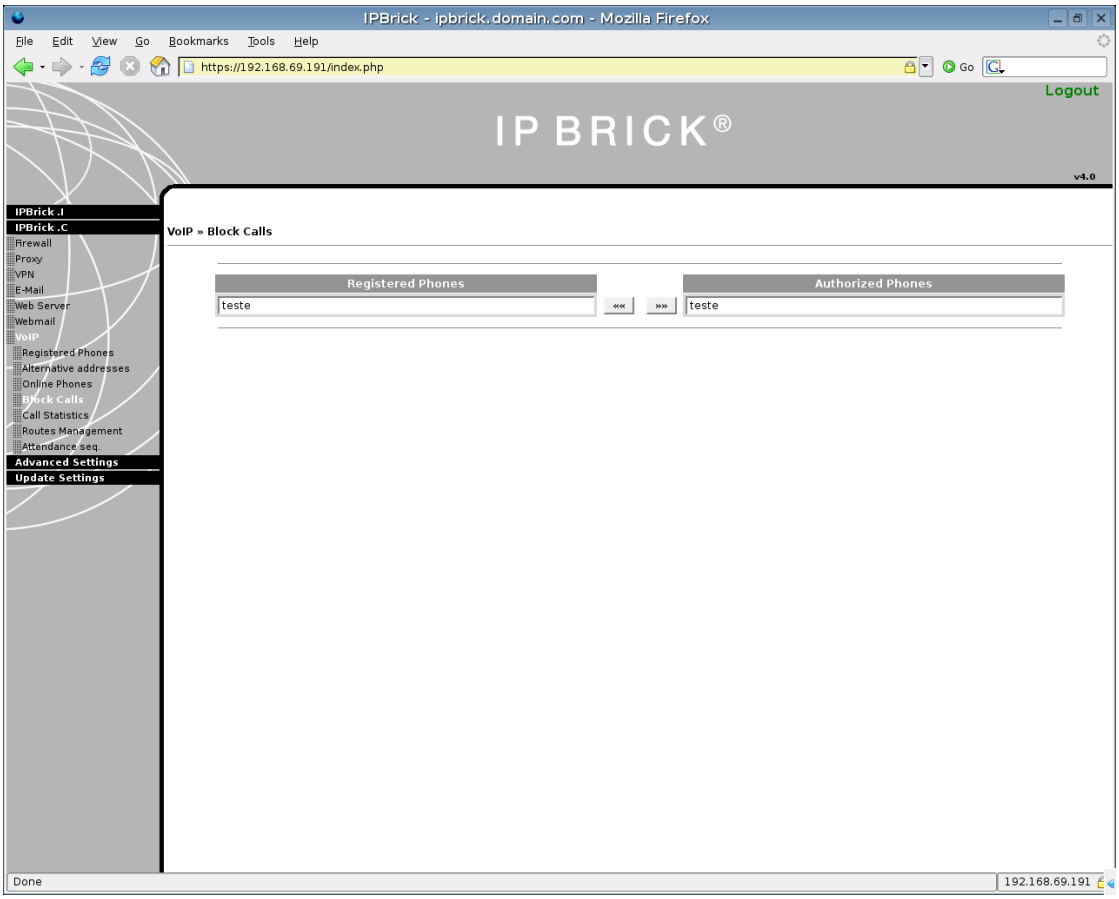

FIG. 4.25 – VoIP - Bloquage d' Appels

4.7.5 Statistiques des Appels

Dans cette section on peut vérifier les appels qui ont été faits et les appels en cours. Concernat les deux situations, on peut voir :

- Nombre total d' appels (effectués ou en cours) ;
- Téléphone ;
- Adresse Origine ;
- Adresse d' arrivée ;
- Début ;
- Fin ;
- Durée.

4.7.6 Gestion des Routes

Dans cette option on peut voir (FIG. 4.26) les `Routes locales` et une `liste d' adresses SIP` configurées dans l' *IPBrick*. Il existe un bouton `Insérer` associé à chacune d' elles et on peut voir leur configuration ci-dessous.

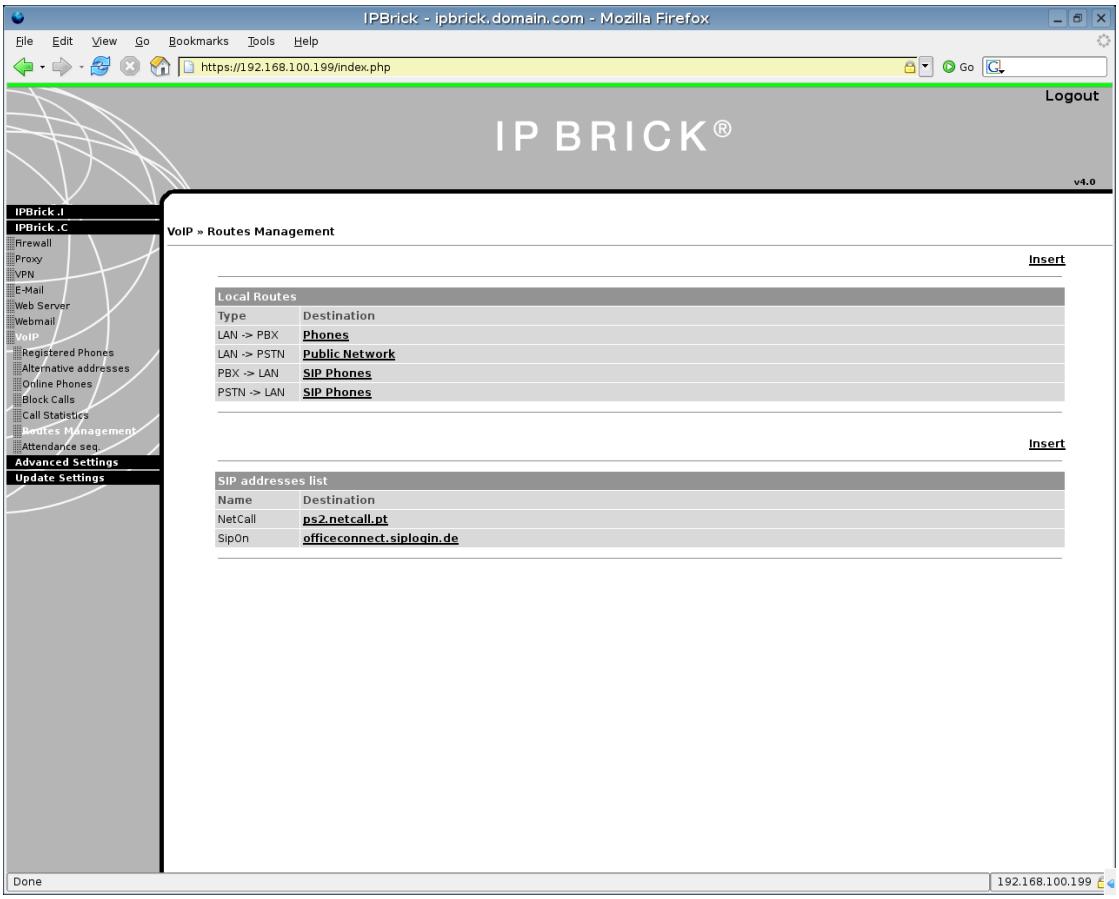

FIG. 4.26 – VoIP - Gestion des Routes

Routes Locales

Les routes locales permettent de traiter les interliaisons du LAN avec le PBX ou le PSTN et il y a 4 types différents :

- `PSTN -> LAN` ;
- `PBX -> LAN` ;
- `LAN -> PBX` ;
- `LAN -> PSTN` ;

En clicant sur le destin de chaque route locale, il est possible de `Modifier`, `Effacer` ou insérer `les Prefixes` que l' on souhaite associer à chaque route.

Liste d' Adresses SIP

Permet de voir la liste d' adresses SIP[14] déjà configurées. En `insérant` une nouvelle adresse, la page créée demande les données suivantes :

- Nom : Nom du Serveur ;
- Adresse du Serveur SIP : adresse IP ou nom du serveur SIP ;
- Proxy RTP[15] : S' il est Actif ou Inactif ;
- Route d' entrée : Indique si c' est une route d' entrée (`Oui`) ou `Non` ;

Ensuite, on doit appuyer sur le bouton Insérer pour que l' adresse soit ajoutée.

4.7.7 Séq. de réponse

La séquence de réponse permet d' indiquer, au cas où l' appel n' est pas pris sur le téléphone principal, quels sont les numéros de téléphones auxquels les appels seront renvoyés.

[14] Session Initiation Protocol
[15] Real Time Protocol

Chapitre 5

Définitions Avancées

Les mens existants dans ce chapitre permettent réaliser les configuretions de plusieurs services. L'organisation de ce chapitre est la suivant :

- IPBrick ;
- Téléphonie ;
- Réseau ;
- Services d'appui ;
- Configuretions ;
- Système.

5.1 *IPBrick*

5.1.1 Définitions

Dans cette section vous pouvez définir quelques conFiguretions essentielles du serveur *IPBrick*.

Dans les `Définitions de Domaine`, vous configurez le nom (hostname) et le domaine DNS du serveur. Le nom complet de la machine est désigné par *Fully Qualified Domain Name* (FQDN)et il est composé par le nom suivi du domaine DNS. Par exemple, si le hostname est '*IPBrick*' et le domaine DNS est **entreprise.fr** e FQDN sera 'ipbrick.**entreprise.fr**'. Pour changer ces définitions, effectuer une clique en `Changer`.

En `Définitions de réseau`, ce vous configurez les propriétés des interfaces de réseau, privé ou public, de l'*IPBrick*. Ces propriétés sont l'adresse IP, masque, adresse de réseau et l'adresse de broadcast.

⇒ **Remarque: L'interface privée est la première plaque de réseau que l'*IPBrick* détecte dans le serveur où elle a été installée. Si le serveur a une deuxième plaque de réseau, celle-ci sera configurée comme interface publique.**

Au cas où l'*IPBrick* fonctionnerait comme le serveur d'intranet (*IPBrick.I*) il faut seulement configurer l'interface privée. Dans ce cas, l'interface public,Dans

ce cas, l'interface public (au cas où le serveur où l'*IPBrick* est installé aurait 2 plaques de réseau) peut rester avec les conFiguretions par défaut et il ne devra pas avoir un câble de réseau. Si l'*IPBrick* fonctionne comme le serveur de communications (*IPBrick.C*) ou s'il accumule les fonctions d'Intranet et de communications (*IPBrick.I + IPBrick.C*), l faut configurer les deux interfaces (dans ces situations le serveur où l'*IPBrick* a été installée devra avoir deux plaques de réseau).

Pour changer les définitions des interfaces de réseau, aire clique en `ETH0` ou en `ETH1`.

En `Route par défaut`, vous devrez définir la passerelle de l'*IPBrick*.

Si l'*IPBrick* fonctionne comme le serveur de l'intranet (*IPBrick.I*), l'adresse a placer dans ce champ est l'adresse de l'équipement qui fait l'accès à l'Internet. Cet équipement pourra être, par exemple, une *IPBrick* de Communications ou un routeur.

! Attention: Dans le cas décrit dessus, l'adresse IP de la passerelle devra être une adresse du même réseau IP configurée dans l'interface privée, l' `ETH0`**. Par exemple, si l'interface privée a l'adresse IP 192.168.1.1, l'adresse IP de la passerelle devra être** `192.168.1.x`**. AL'interface à choisir pour configurer la passerelle est** `ETH0`**.**

Si l'*IPBrick* fonctionne comme le serveur de Communications (*IPBrick.C*) ou si elle a fonctions d'Intranet et de Communications (*IPBrick.I+ IPBrick.C*), l'adresse a taper dans ce champ est l'adresse de l'équipement qui fait l'accès à l'Internet, par exemple, un routeur.

! Attention: Dans le cas décrit dessus, l'adresse IP de la passerelle devra être Un adresse du même réseau IP configurée dans l'interface publique, `ETH1`**. L'interface à choisir pour configurer la passerelle é** `ETH1`**.**

Pour changer la définition de la passerelle, faire une clique en `Changer`.

5.1.2 Informations du système

L'information présentée dans ce page a un résumé de la configuretion de l'*IPBrick*, le temps d'activité de la machine (dès la dernière fois qu'elle a été initialisée), volume de trafic dans les interfaces physiques (ETH0 e ETH1) et logiques, caractéristiques du hardware du serveur et les taux de l'occupation de mémoire et les partages du disque dur du serveur.

5.1.3 Accès

Cette section permet changer les donnés d'accès à l'*IPBrick*. Les dés d'accès, par défaut, pou accéder à *IPBrick* par l'interface web sont :

– Login : administrador
– Mot de passe : 123456

Le login administrateur et son mot de passe concernent, seule et exclusivement, à l'authentification à utiliser pour accéder à l'*IPBrick* par l'interface web et les

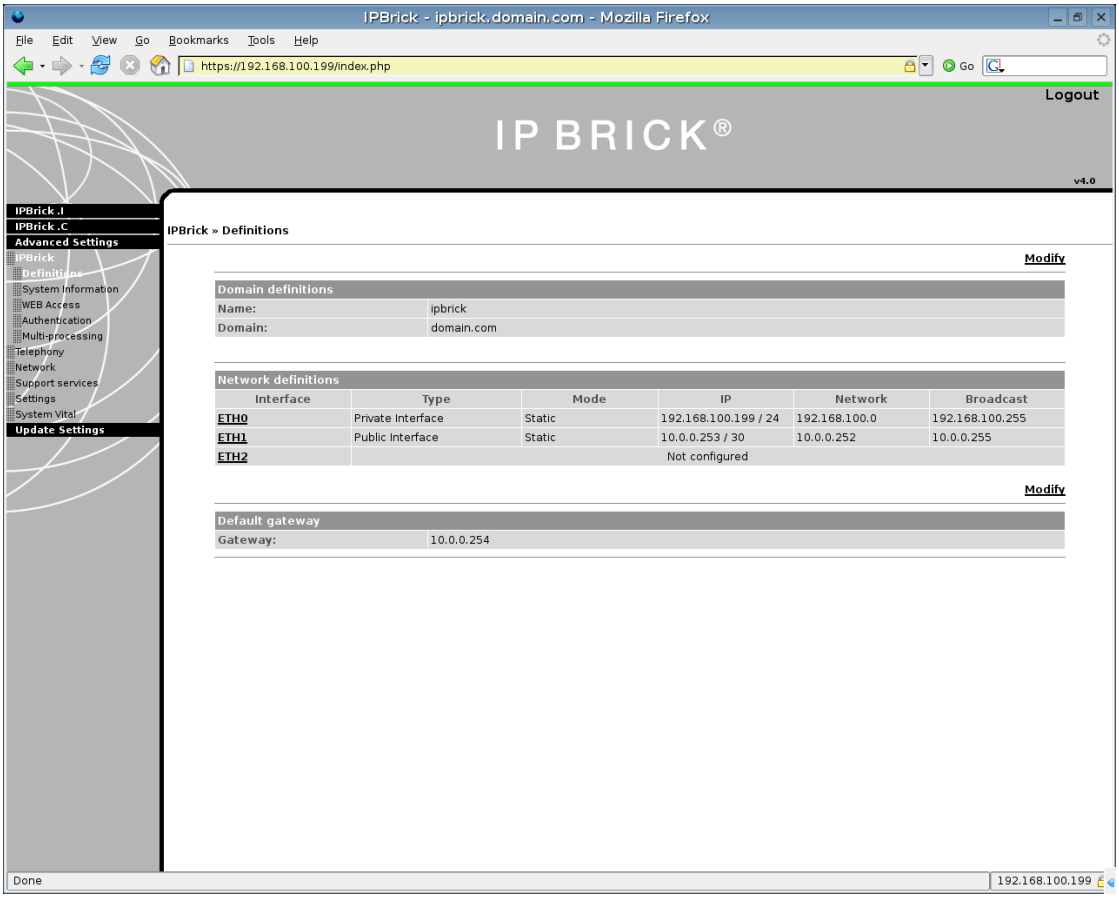

FIG. 5.1 – Définitions de l'*IPBrick*

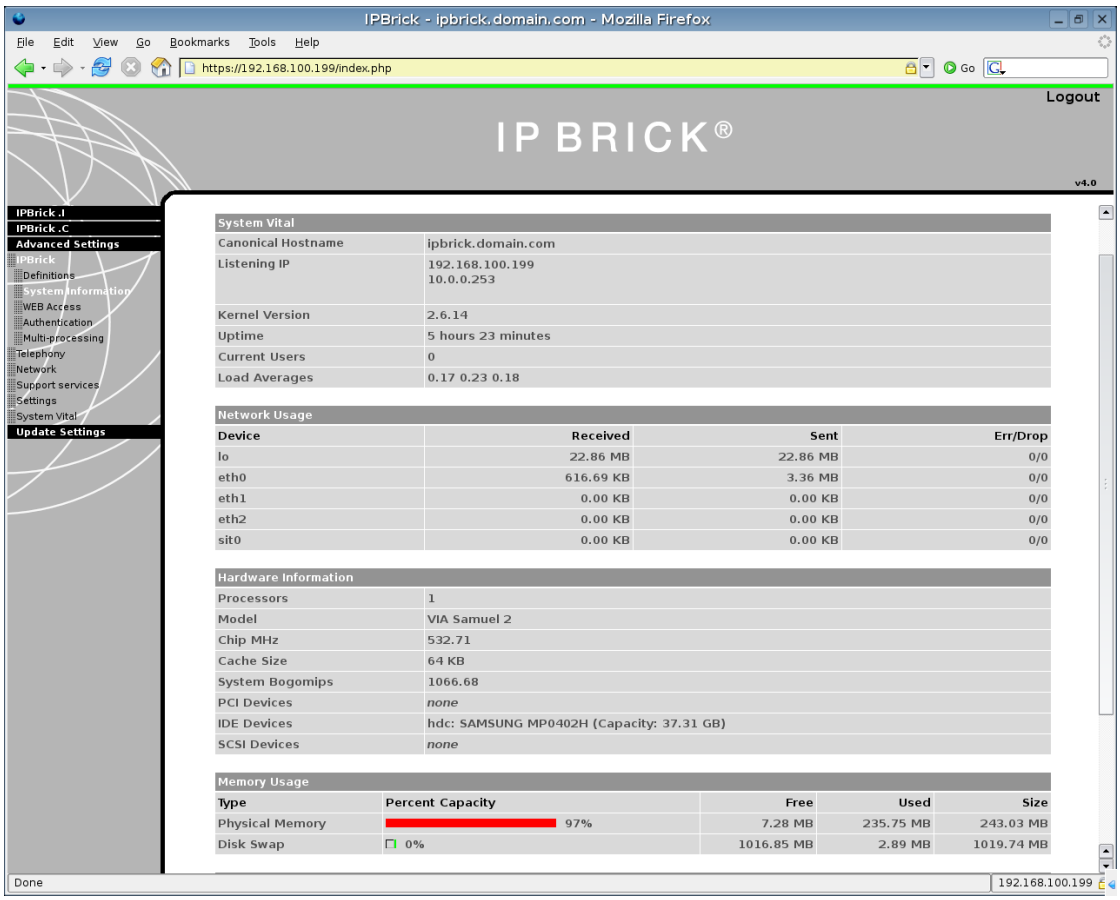

FIG. 5.2 – Informations du système

deux peuvent être changés.

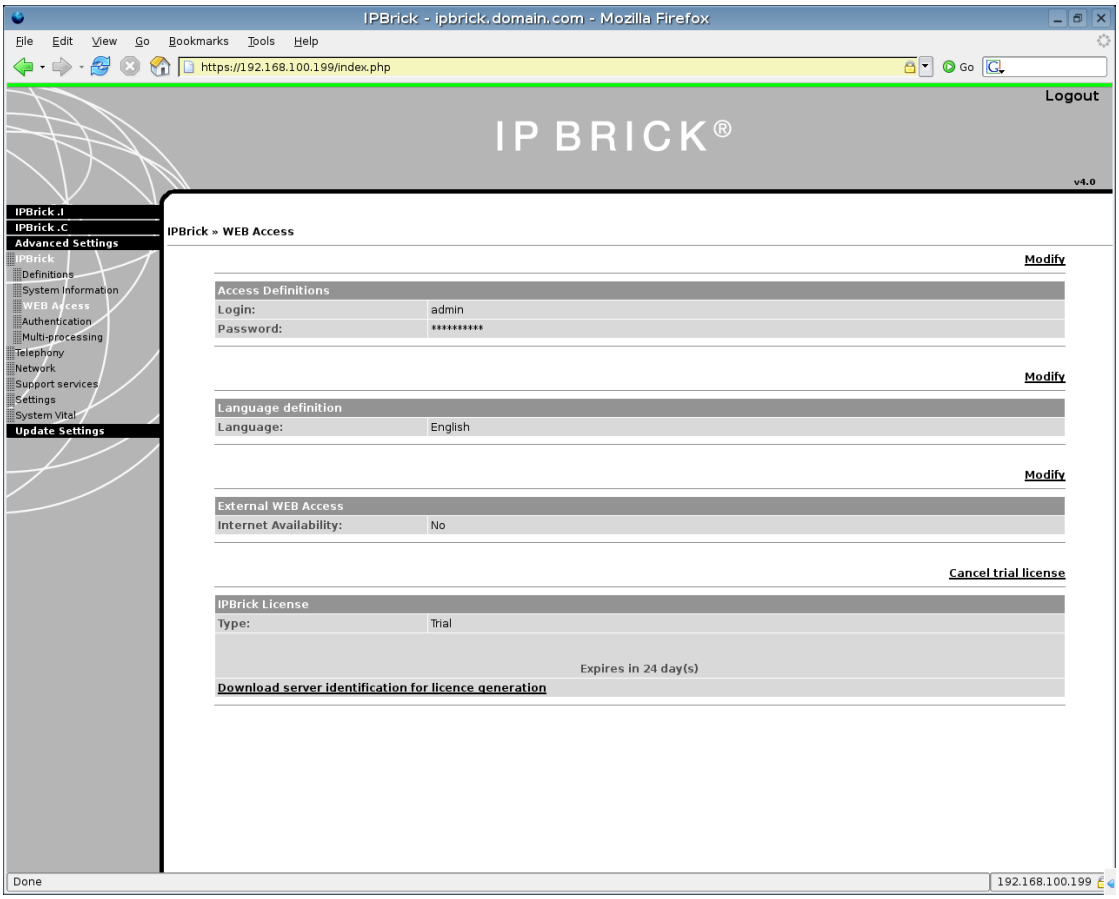

FIG. 5.3 – Login d'accès

⇒ **Remarque: Au contraire de l'utilisateur `Administrator`, ce login administrateur n'a pas une aire de travail crée dans l'*IPBrick*.**

L'*IPBrick* est actuellement disponible en 5 langues :

- Portugais ;
- Anglais ;
- Espagnol ;
- Français ;

Cette section permet de changer l' idiome de l' *IPBrick*. Afin d' effectuer ce changement , il faut juste cliquer sur `Modifier`, sélectionner l' idiome souhaité et ensuite cliquer sur `Actualiser Définitions`.

Si on veut accéder à l' interface de configuration de l' *IPBrick*à travers de l' Internet (`Accès Web Externe`), on doit cliquer sur `Modifier` et choisir `OUI`. Il est aussi indispensable d' activer le service HTTPS pour l' Internet. Il faut cliquer sur `Actualiser Définitions` pour que les changements soit faits.

C' est aussi sur cette page que l' on peut actualiser la licence de l' *IPBrick*. Si vous avez une licence expérimentale, cliquez sur "Download du fichier à envoyer" et envoyer le fichier - vers `support.ipbrick@iportalmais.pt`. Aprés avoir reçu la réponse (avec un fichier annexe) de **iPortalMais**, annulez la Licence Temporaire et sur la page crée vous pouvez insérer le fichier reçu, devenant la licence expérimentale une Licence Permanente.

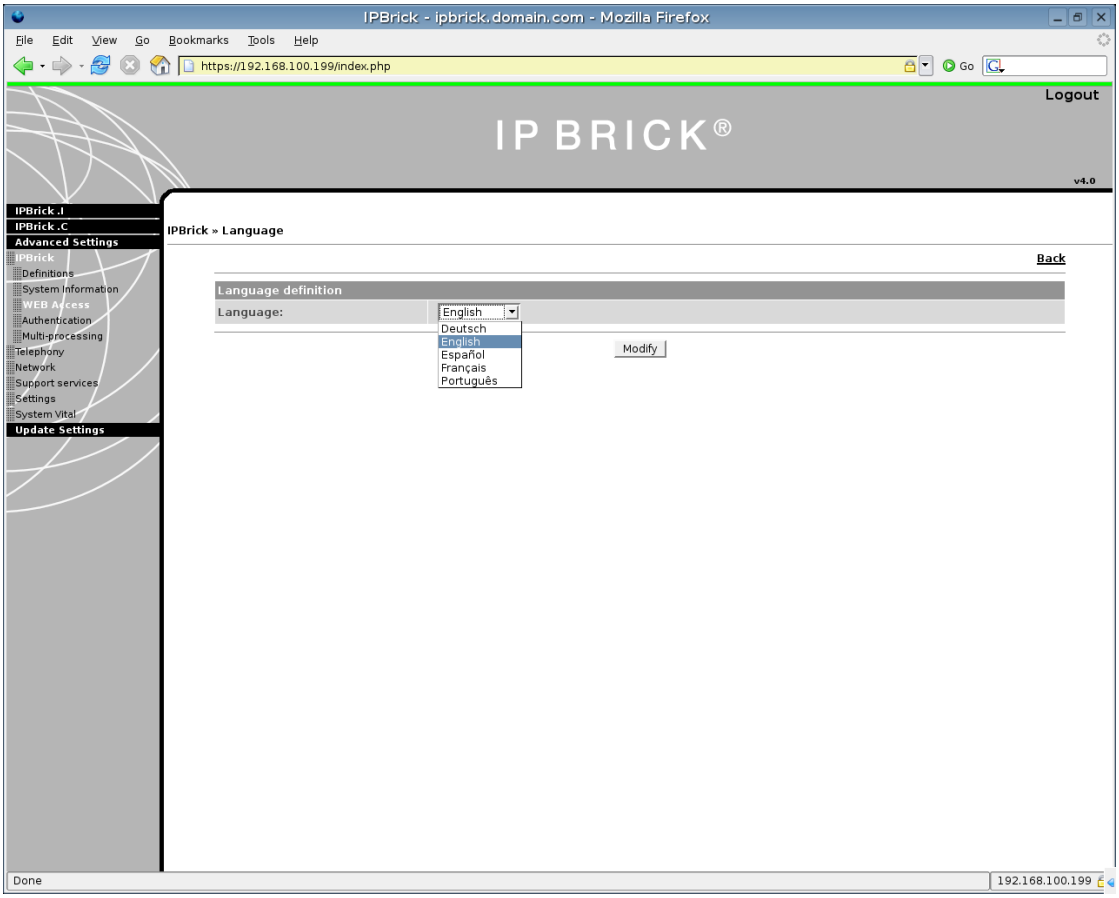

FIG. 5.4 – Idiome

5.1.4 Authentification

Cette section est particulièrement importante, car votre configuretion détermine la façon de faire les authentifications des services disponibles par l'*IPBrick*, comme par exemple, le service du courrier électronique.

Si un utilisateur veut lire votre messages du courrier électronique, il a besoin d'avoir le nom de l'utilisateur et le mot de passe que lui permet faire l'authentification. Dans cette section, on définie où l'*IPBrick* va vérifier les donnés des utilisateurs pour garantir ou empêcher l'accès.

L'*IPBrick* pourra vérifier les donnés de l'utilisateur localement ou externe, dans un autre serveur.

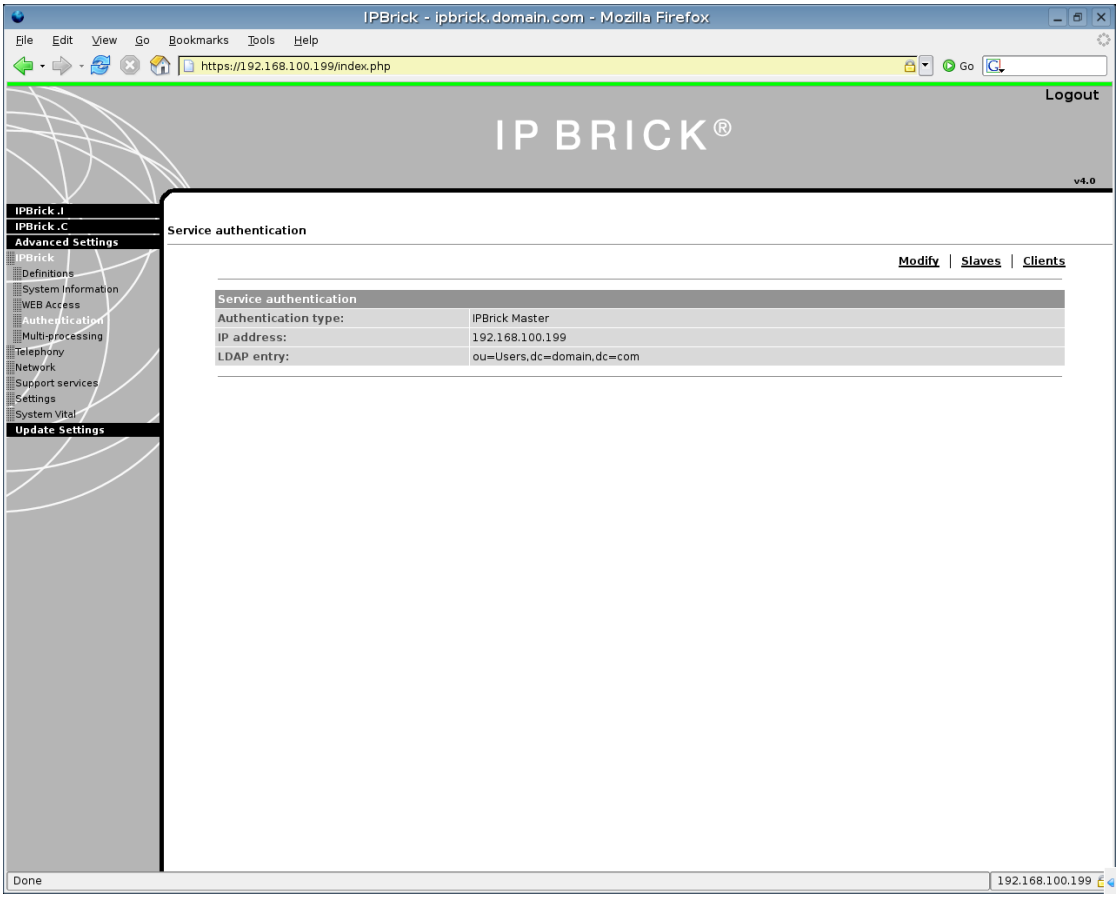

FIG. 5.5 – Authentification

Les options de l'authentification disponibles sont les suivantes :

1. Master *IPBrick* : l'authentification est faite dans le propre *IPBrick*. S'il y a un autre serveur d'authentification, cet *IPBrick* sera le serveur d'authentification principale (Master) ;
2. Slave *IPBrick* : l'authentification est faite dans l' *IPBrick*, mais l' *IPBrick* n'est pas un serveur d' authentification principal ; il est un serveur d' authentification secondaire, en synchronisant sa base de données des utilisateurs avec le *IPBrick* ;
3. Client *IPBrick* : dans ce genre d' authentification, le client utilise un serveur *IPBrick* pour faire son authentification, ne possédant pas la base des utilisateurs ;
4. Client Netbios : permet la compatibilité avec les serveurs Windows NT ;
5. Membre d' un Domaine AD (Master *IPBrick*) : dans ce cas-là, l' IPBrick fait partie d' un domaine AD, et possède une copie de la base de données des utilisateurs ;
6. Membre d' un Domaine AD (Slave *IPBrick*) : l' IPBrick fait aussi partie du domaine, synchronisant sa copie de la base de données des utilisateurs avec le Master IPBrick, qui est aussi membre du même domaine.

! Attention: Après changer la façon d'authentification de l'*IPBrick*, au `Actualiser Définitions`, l'*IPBrick* va re-initier automatiquement.

L'option `Master IPBrick` doit être choisie en deux situations :

– Il y a seulement un *IPBrick* dans l'entreprise et les utilisateurs ont étés enregistrés dans l'*IPBrick* ;
– Il y a deux ou plusieurs *IPBrick* dans l'entreprise mais, cet *IPBrick* sera le serveur d'authentification principale (Master). Dans ce cas, c'est nécessaire d'indiquer les serveurs secondaires (Slaves). Pour cela, cliquer sur `Slaves` et indiquer le nom ou l'adresse IP pour chaque serveur secondaire.

L'option `Slave IPBrick` doit être choisie seulement quand :

– Il y a autre *IPBrick* dans l'institution qui est configurée comme LDAP Locale (Master). Dans ce cas, il n'est pas possible d'enregistrer les utilisateurs dans l'*IPBrick* configuré avec LDAP Locale. C'est seulement nécessaire indiquer le nom ou l'adresse IP de l'*IPBrick* configuré comme Master (LDAP Locale).

L'option `Membre d' un Domaine AD` sera celle que vous voulez quand :

– l y a un serveur Windows dans l'entreprise qui possède déjà un registre de tous les utilisateurs. Dans ce cas, il n'est pas nécessaire d'enregistrer utilisateur dans l'*IPBrick*. Pour configurer la façon d'authentification WinServer sont précises les suivantes données :

  1. Adresse IP du serveur du domaine Windows ;
  2. Nom du domaine ;
  3. Nom de l'utilisateur et le mot de passe d'un utilisateur du domaine lointain avec permissions de l'administrateur ;
  4. Administrateur DN ;

5. Base DN de recherche d'utilisateurs ;
6. Base DN de recherche de groupes.

⇒ **Remarque: Pour organiser et garder les informations des utilisateurs, l'*IPBrick* utilise *Lightweight Directory Access Protocol* (LDAP). LDAP est un service de directoire où vous pouvez garder toute les informations d'une entreprise utilisateurs, ordinateurs, contacts, imprimantes, etc.**

Pour obtenir plus informations et exemples de configuretion, consulter le *Manuel d'Utilisation de IPBrick*.

5.1.5 Multitraitement

Les ordinateurs plus récents possèdent plusieurs processeurs (virtuels ou physiques). Pour profiter de ces processeurs, il faut activer le support multitraitement, voir FIG. 5.6. Aprés avoir activé cette fonction, le système démarrera avec un Kernel du type SMP[1].

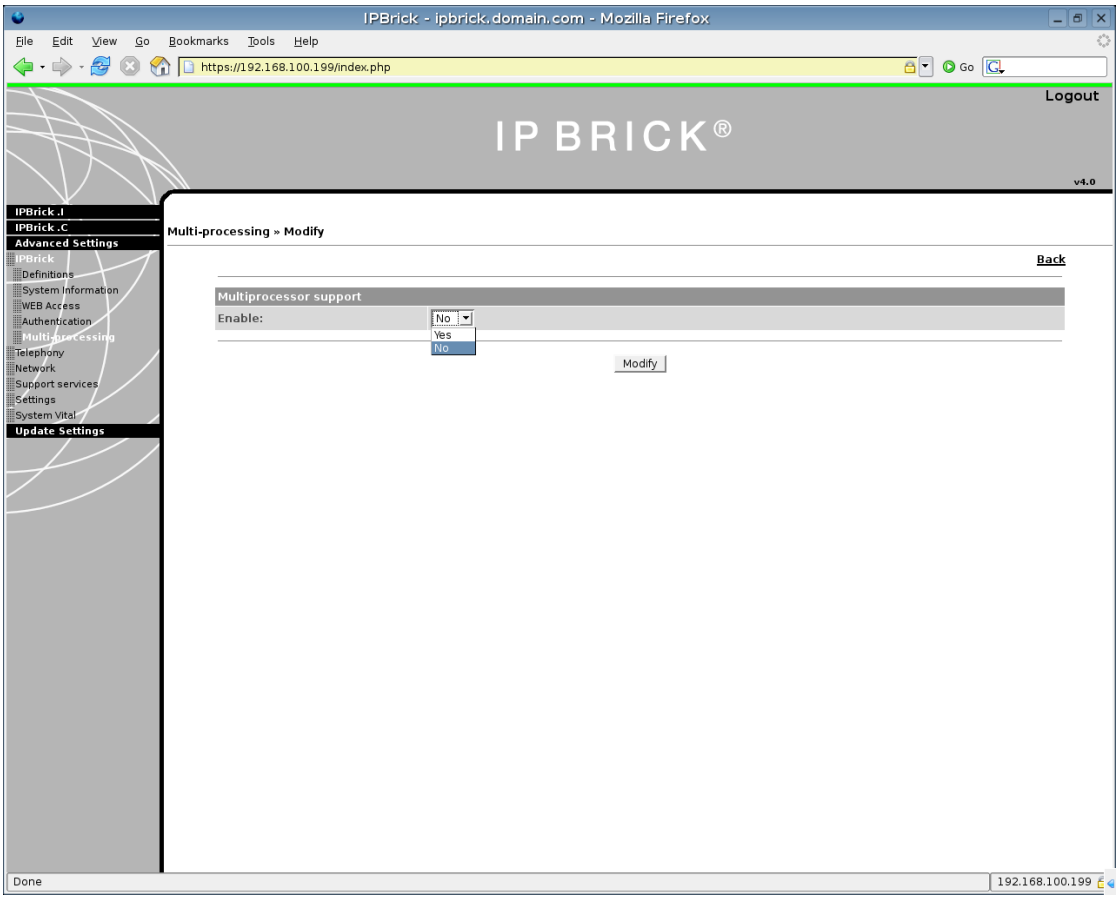

FIG. 5.6 – Multitraitement

[1]Symmetric MultiProcessor

5.2 Téléphonie

Dans cette section (`Définitions Avancées` » `Téléphonie`), il est possible de configurer des plaques RDIS BRI, RDIS PRI ou ANALOGIQUES.

Aprés leur configuration physique[2] il faut faire la configuration dans l'*IPBrick*. Pour pouvoir faire cette configuration il faut savoir comment a été faite la configuration physique de la plaque, c'est-à-dire, la configuration de chaque porte. Pour insérer il faudra choisir la liaison `Insérer` et, ensuite indiquer Fig. 5.7) :

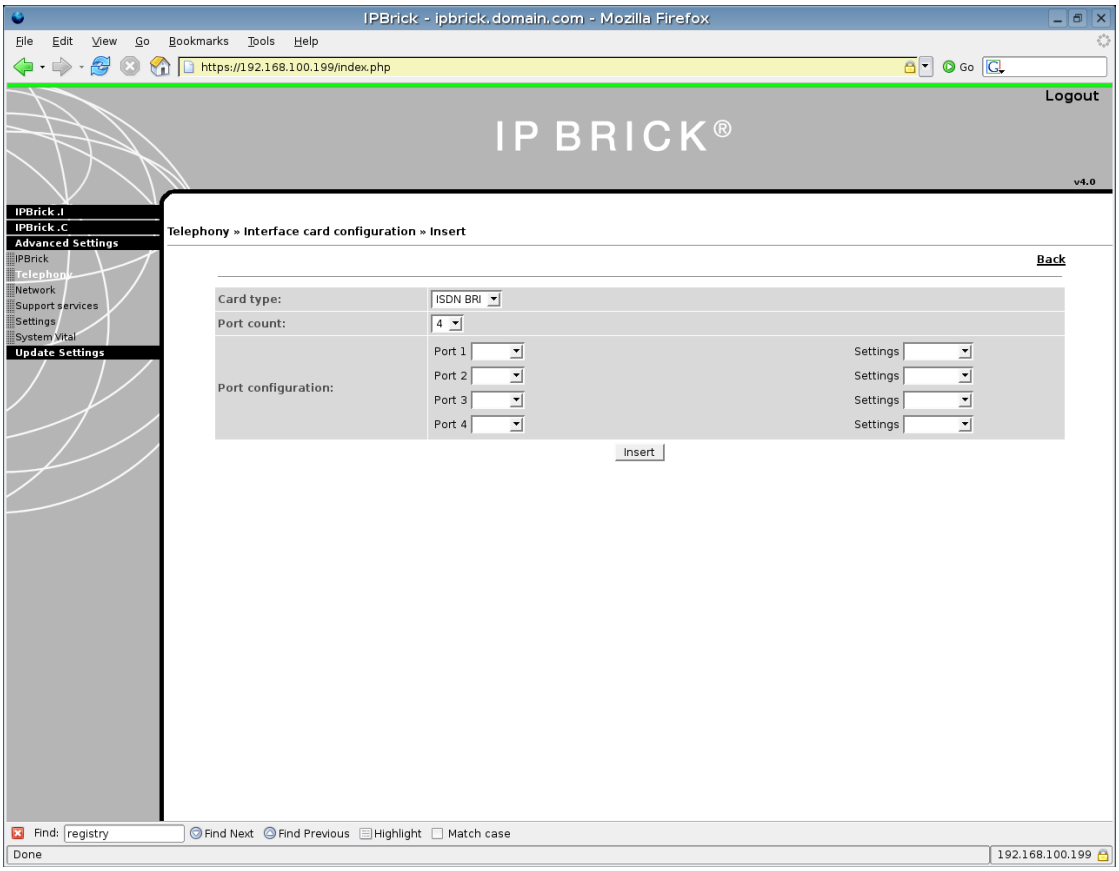

Fig. 5.7 – Téléphonie - Insérer

- Type de Plaque :
  - Analogique ;
  - RDIS BRI ;
  - RDIS PRI.
- Nombre de Portes : 1, 2, 4, 8, etc (selon le type de plaque) ;
- Configuration des Portes :
  - Porte :
    - PSTN ;
    - PBX.

[2]Voir *Manuel d' Installation IPBbrick.GT*

- Configuration :
  - NT PtP (Point to Point) ;
  - NT PtMP (Point to Multi-Point) ;
  - TE PtP (Point to Point) ;
  - TE PtMP (Point to Multi-Point).

Le bouton `Insérer` confirme l' addition de la nouvelle plaque.

Aprés avoir configuré la plaque, en accédant aux `Définitions Avancées` » `Téléphonie`, la liste avec les plaques configurées apparaît, comme on peut vérifier sur FIG. 5.8.

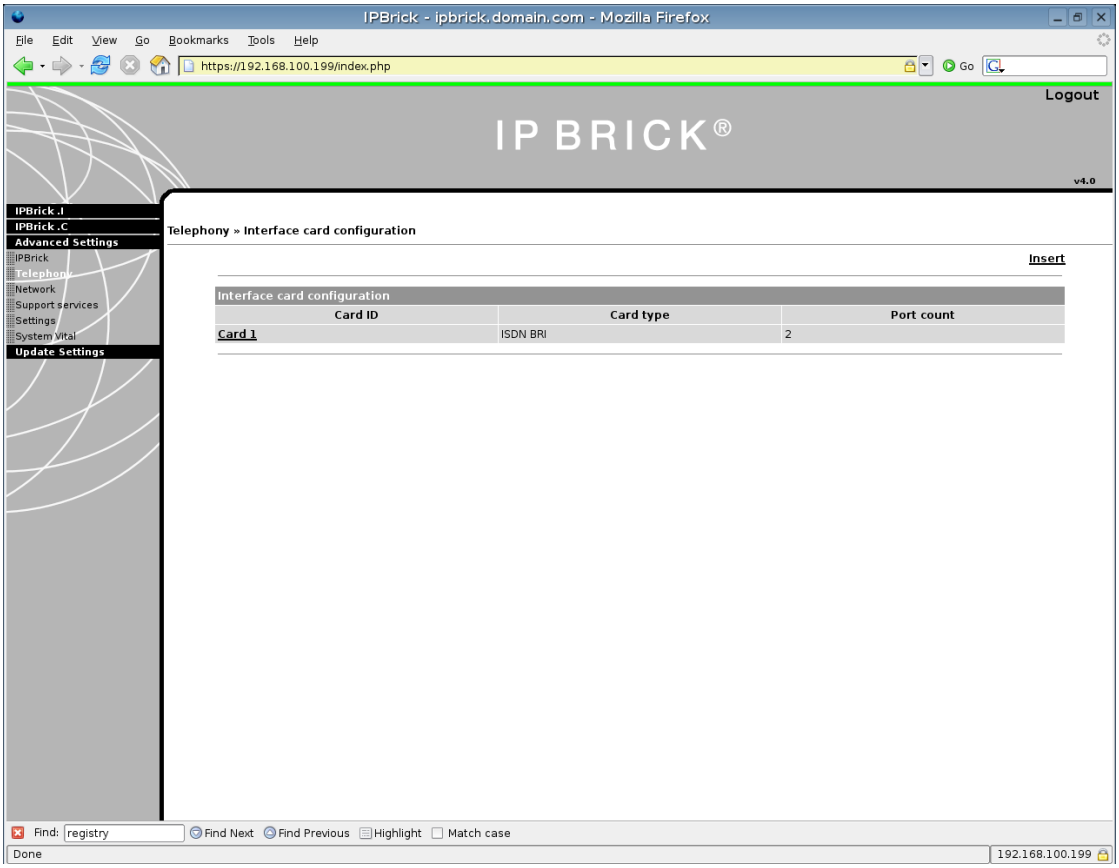

FIG. 5.8 – Téléphonie

5.3 Réseau

Configuretion de services rapportés avec la structure du réseau de l'entreprise. Ici vous définissez les règles personnalisées de pare-feu, vous indiquez des itinéraires pour autres réseaux internes (ou externes) et vous définissez des règles et des priorités dans le service de QoS[3].

[3]Quality of Service

5.3.1 Pare-feu

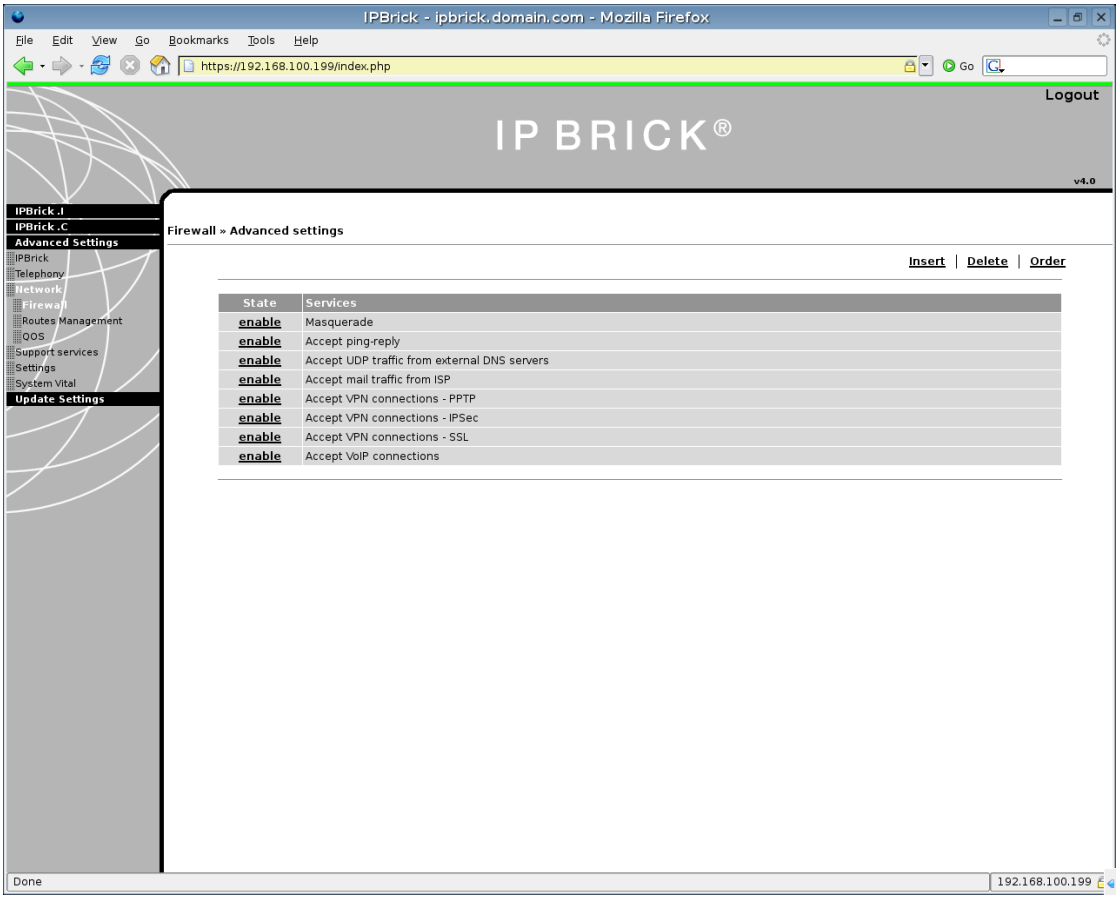

FIG. 5.9 – Réseau - Pare-feu

Présentation

Dans cette section, nous traitons de la gestion du pare-feu de *IPBrick*. Dans la section de pare-feu de *IPBrick* nous avons déjà présenté quelques règles prédéfinis, elles ne peuvent pas être modifiés par l'utilisateur, mais elles peuvent être désamorcées. Néanmoins, autres règles sont exigées par la conFiguretion de quelques services celles-ci dans la section `Commander` pourront être en partie *gérées* par l'utilisateur. Ainsi, *IPBrick* offre à son administrateur cette interface avancée de gestion de pare-feu où vous pouvez définir une série de règles avec un niveau de personnalisation suffisamment élevé

Menu Dessus

Connexions pour :

1. `Insérer` : de nouvelles règles dans manière avancée ;
2. `Effacer` : règles déjà insérées ;

3. `Ordonner` : interface d'ordre de toutes les règles présentes dans le pare-feu.

La création de nouvelles règles peur être de trois sortes, à savoir :

- Règle Dnat : permet de faire le NAT[4] ;
- Restriction d' une machine IP : permet de restreindre le trafic d' un ensemble ip/porta ;
- Configuration Générale : permet d' insérer des règles générales, qui on besoin de :
  - Règle :
    - INPUT : les données reçues par le firewall, indépendemment de leur origine ;
    - OUTPUT : donées envoyées par le firewall ;
    - FORWARD : permet le passage de trafic d' une interface à une autre ;
    - PREROUTING : pour des paquets qui viennent de l' internet et accèdent à un serveur avec un ip privé ;
    - POSTROUTING : pour des paquets qui vont vers l' internet, dont l' adresse ip d' origine (privé) est échangée par l' adresse ip publique.
  - Interface : choisir l'interface à laquelle on veut appliquer la règle ;
  - Protocole : le protocole (ou tous) auquel on veut appliquer la règle ;
  - Module :
  - Ip Origine : adresse ip d' origine du paquet ;
  - Port d' Origine : port d' origine du paquet ;
  - Ip d' arrivée : adresse ip d' arrivée du paquet ;
  - Port d' Arrivée : port d' arrivée du paquet ;
  - Identificateur : nom de la règle ;
  - Politique :
    - ACCEPTER : Permet d' accepter un paquet et le laisser passer pas les règles du firewall ;
    - DROPPER : N' accèpte pas le paquet, et il est effacé ;
    - MARK : permet de garder une marque dans le paquet. Ces marques peuvent être utilisées pour prendre des décisions au niveau du renvoi des paquets ;
    - LOG : garde un log de tous les paquets qui suivent la règle.

Corpus

Liste de toutes les règles contrôlées par l'utilisateur. Une règle peut être alternée entre son état `Actif` et `Inactif`. Il n'est pas possible de modifier/réécrire une règle, pour faire ça, vous devrez effacer la règle concernée et ensuite vous insérerez une nouvelle.

Afin d' éliminer les règles, cliquer sur `Effacer`, sélectionner la règle ou les règles à éffacer et appuyer sur le bouton `Effacer`. Les règles qui sont définies par défaut ne peuvent pas être effacées, mais peuvent, cependant, être desactivées.

[4]Network Address Translation

5.3.2 Gestion de Routes

Présentation

Quand une entreprise a plusieurs réseaux distribués et séparés par plusieurs routeurs, si vous voulez qu'*IPBrick* soit accessible à ces réseaux, vous devrez ici indiquer le route (rompue) pour ces réseaux. (Fig. 5.10)

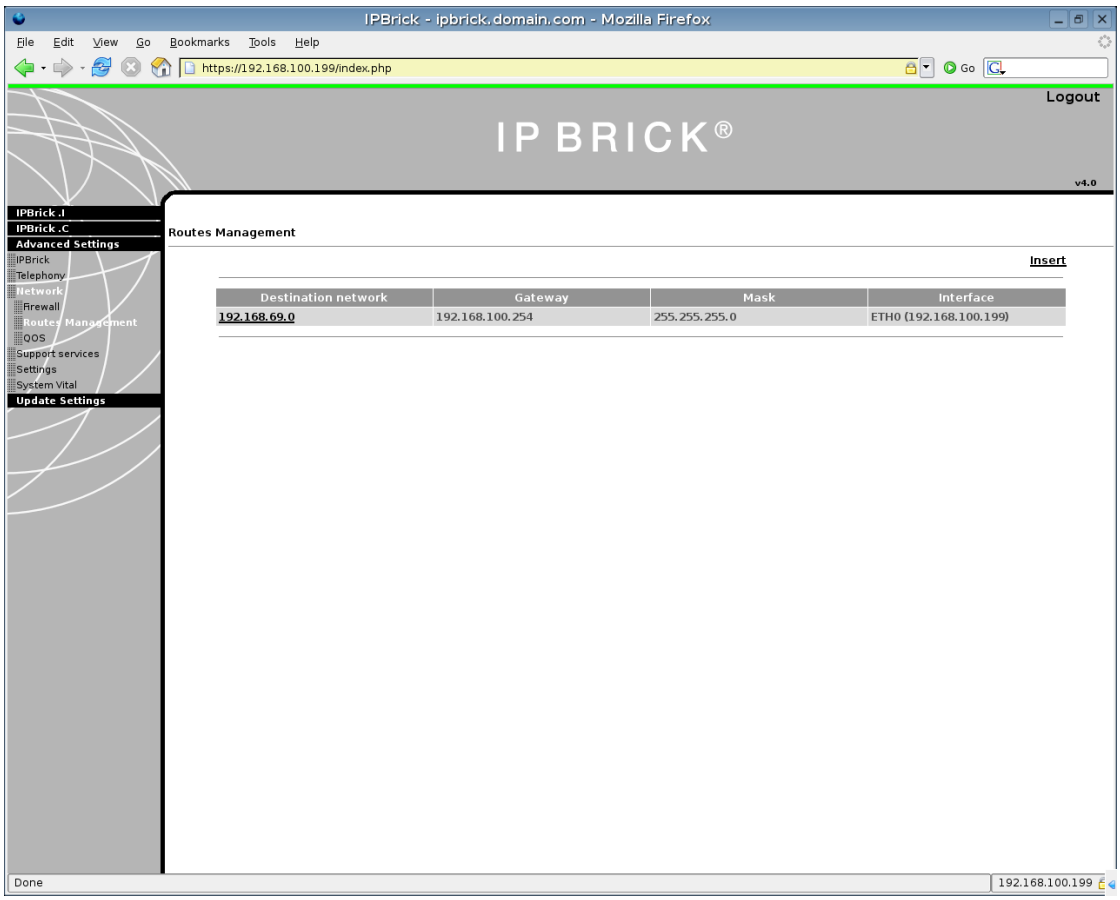

Fig. 5.10 – Réseau - Gestion de Routes

Menu Dessus

Connexion Pour `insérer` une nouvelle route, où nous indiquerons le filet IP de destination et le respectif masque ainsi que l'IP du routeur qui fait cette connexion. Vous devez aussi indiquer l'interface de réseau qui est lié au réseau du routeur indiqué.

Corpus

Liste des routes introduites.

5.3.3 QoS

Présentation

Ce service (Fig. 5.11) de *IPBrick* a comme but garantir un correctement niveau de qualité du service pour l'utilisateur final. Pour ça, on appelle l'attention pour l'importance d'indiquer la valeur de la largeur de bande disponible dans la connexion pour l'Internet. À partir de ces données, vous réussissez à établir des règles de priorité entre les plusieurs types de trafic dans un réseau Par exemple : à l'inverse d ?avoir la connexion à l'Internet complètement occupé par emails, parce que ne limitera pas la largeur de bande attribuée à ce service et garantir un minimum pour le trafic Web !

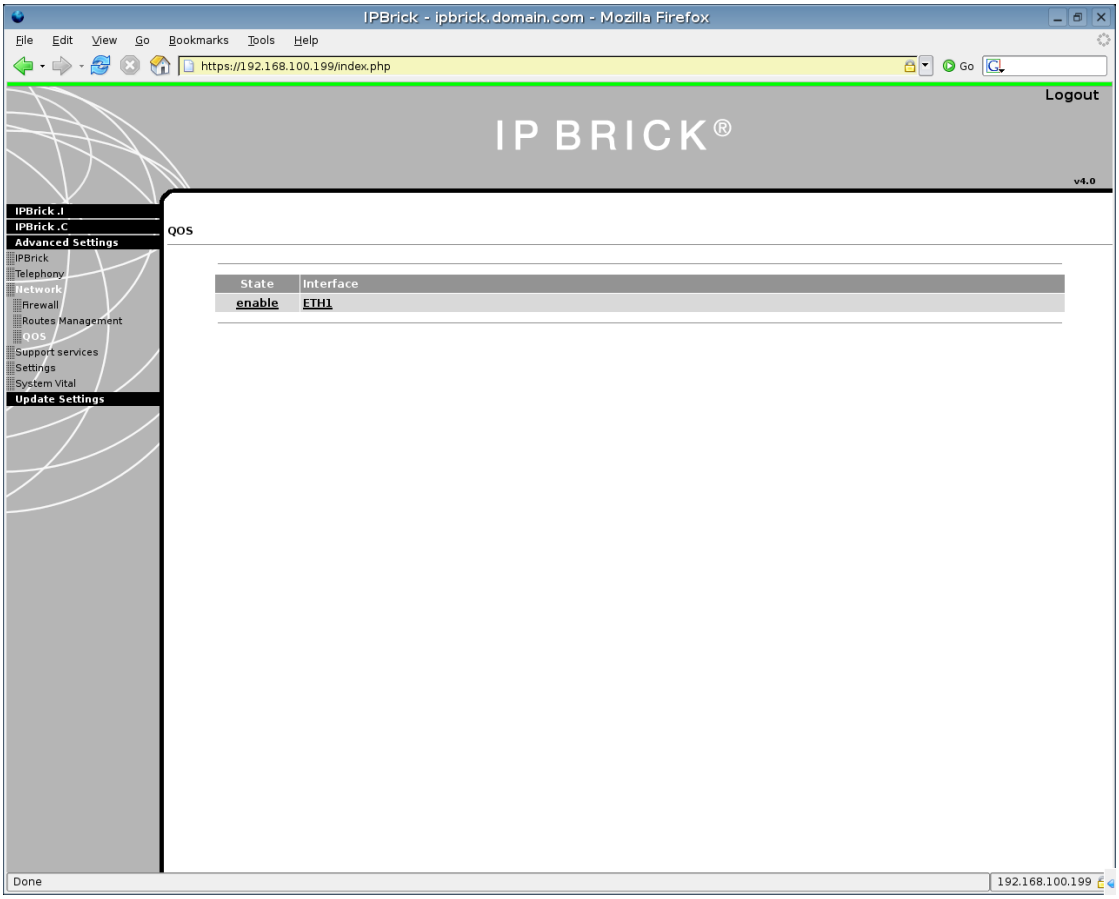

Fig. 5.11 – Réseau - QoS

Corpus

Liste des `Interfaces Publiques` disponibles (normalement sera seule `ETH1`) et de l'état du service pour chaque plaque de réseau. Cliquant dans l'état nous pouvons transiter entre `actif` et `inactif`. Cliquant dans l'état nous pouvons transiter entre actif et inactif. (Fig. 5.12)

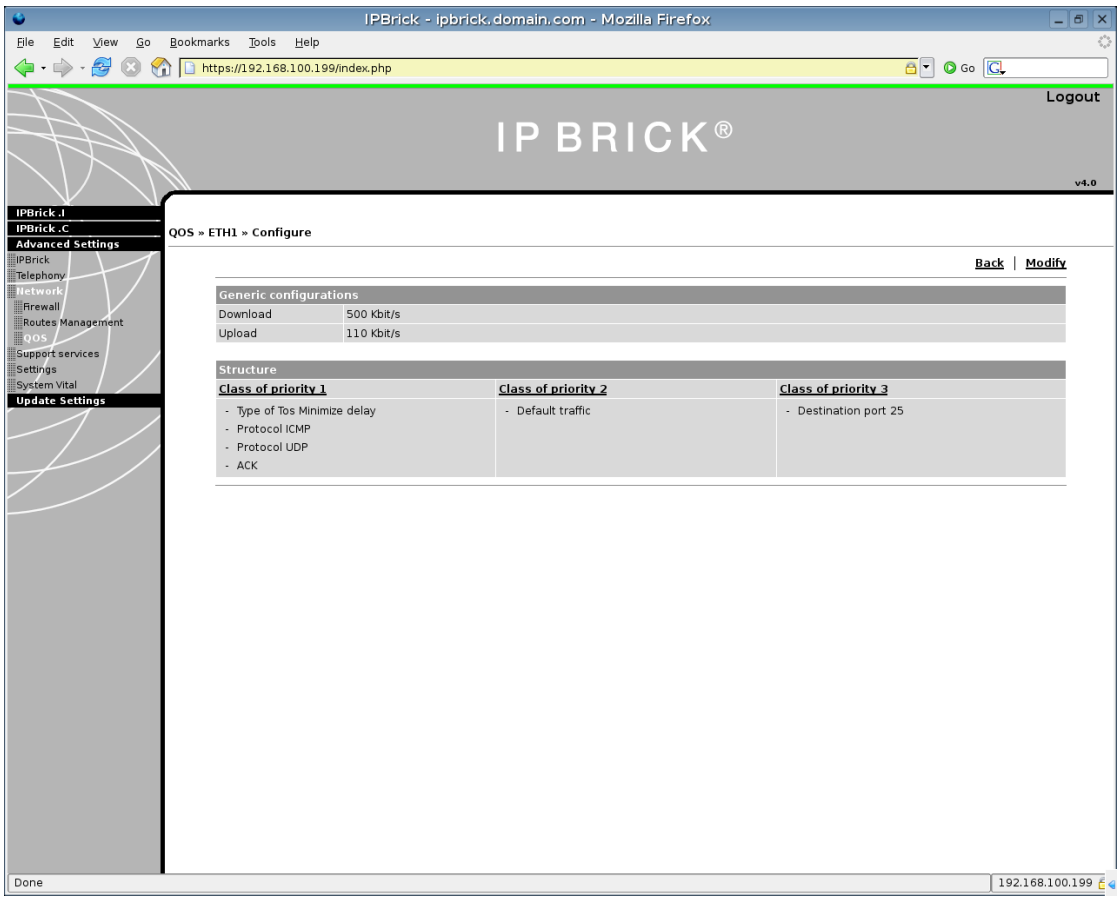

FIG. 5.12 – Réseau - Gestion QoS

5.4 Services d'appu

5.4.1 Gestion de machines

Cette section est la version avancée de la gestion de machines du menu de *IPBrick.I*. Cette interface permet d'ajouter, de modifier ou d'enlever le registre de machines.

Dans la présente version de *IPBrick*, cette section permet d'ajouter des machines au domaine. seule fois, vous devez utiliser la section de la gestion de machine du menu *IPBrick.I*(section 3.1).

5.4.2 DNS

Présentation
Celle-ci est la principale section de configuretion de DNS (Fig.5.13). ACelle-ci est la principale section de conFiguretion de DNS. Modifier des registres de machines, donc (`CNAME`), registres `MX`[5].

Menu Dessus
Connexion Pour `insére` nouveau domaine. (Fig. 5.14)

Corpus
Liste des plusieurs zones de résolution directe et inverse enregistrées à *IPBrick*. Cliquant dans une de ces zones vous accédons à son interface de gestion (Fig. 5.15)

Domaines

Insérer Zones

Menu Dessus
Connexion `Tourner` à liste précédente et ainsi annulera à nouveau l'introduction en cours.

Corpus
Formulaire de registre de zones de résolution directe et/ou inverse, les champs présentés sont :

1. `Domaine` : est la dénomination du nouveau registre, ex : `empresa.pt` ; `porto.empresa.pt` ; `acme.inc` ;
2. `Réseau` : IP associé pour que laquelle vous pourrez créer les registres de résolution inverse PTR[6] ;

[5]Mail Exchange record - Menu Dessus Connexion Pour insérer nouveau domaine.
[6]Pointer, ou pointeur

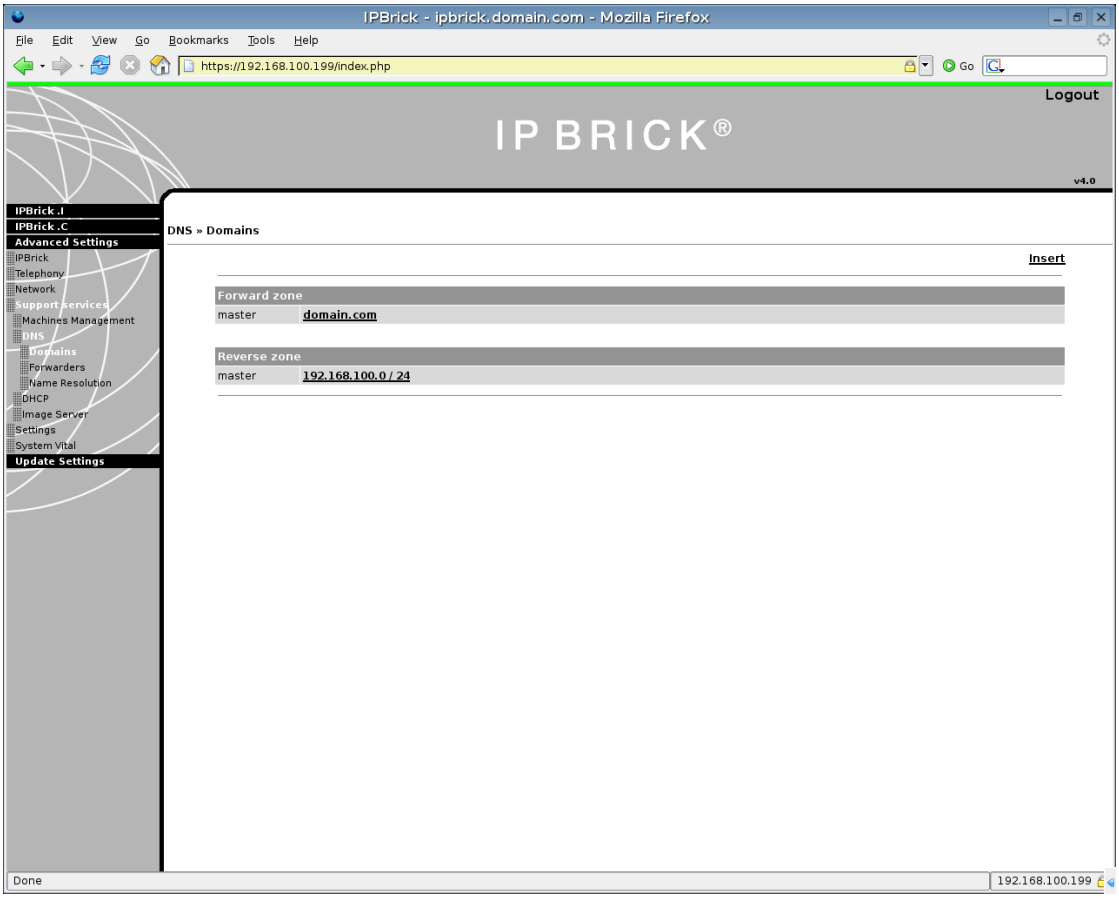

FIG. 5.13 – DNS - Domaines

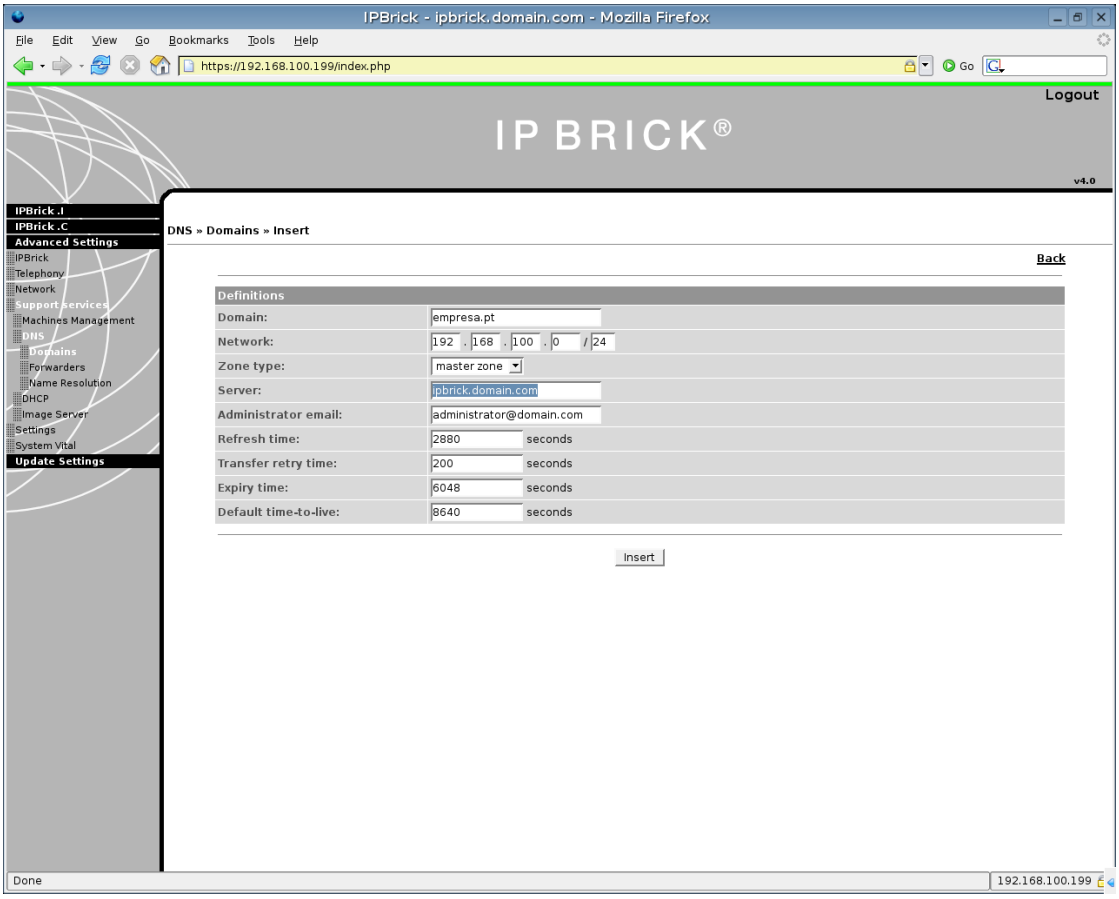

FIG. 5.14 – DNS - Insérer Zones de résolution directe et inverse

3. `Façon de zone` : Elle permet de créer une zone primaire ou secondaire. Une zone secondaire est une copie d'une zone primaire définie dans autre serveur de DNS ;
4. `Serveur` : est nom de la machine où ce domaine sera servido[7] (exe :`ipbrick.domain.com`). (Ce champ seulement s'applique si la zone est du type primaire) ;
5. `Email du responsable` : de ce domaine. Dans DNS celui-ci est le mail enregistré du responsable technique de ce domaine. (Ce champ seulement s'applique si la zone est du type primaire) ;
6. `Temps de rafraîchissement` : est l'intervalle de temps que un secondaire doit utiliser pour vérifier des modifications dans la primaire. (Ce champ seulement s'applique si la zone est du type primaire) ;
7. `Temps entre de nouvelles tentatives` : est le temps que un secondaire doit attendre pour tourner contacter le primaire cas ne l'ait pas réussi dans la dernière tentative de rafraîchissement. (Ce champ seulement s'applique si la zone est du type primaire) ;
8. `Temps d'expiration` : est le temps depuis la dernière tentative de rafraîchissement effectuée avec succès qu'un secondaire doit considérer les données de la zone valables. (Ce champ seulement s'applique si la zone est du type primaire) ;
9. `Valable par défaut` : est le temps que les autres serveurs de DNS doivent considérer les données de cette zone valables. (Ce champ s'applique seulement si la zone est du type primaire)
10. `Serveurs Master` : c'est l'IP du serveur primaire de cette zone. (Ce champ seulement s'applique si la zone est du type secondaire)
11. `Bouton Insérer` : Insérer dads ;

Gestion de domaines

Présentation

Dans cette section, nous contrôlons tous les registres DNS afférents à la zone sélectionnée.

Menu Dessus

Connexions Pour `tourner` à la liste des zones et visionner quelques données du Domaine sélectionné, vous pouvez modifier ou effacer son registre.

Corpus

Liste des plusieurs sections de DNS, à savoir :

1. `Machines`, adresses de machines dans le présent domaine (un nom associé à un IP - machine). exe :

```
myipbrick   ->  192.168.2.1
```

[7]Start of Authority - Celui-ci est le registre dans DNS à laquelle est associé le serveur ici indiqué

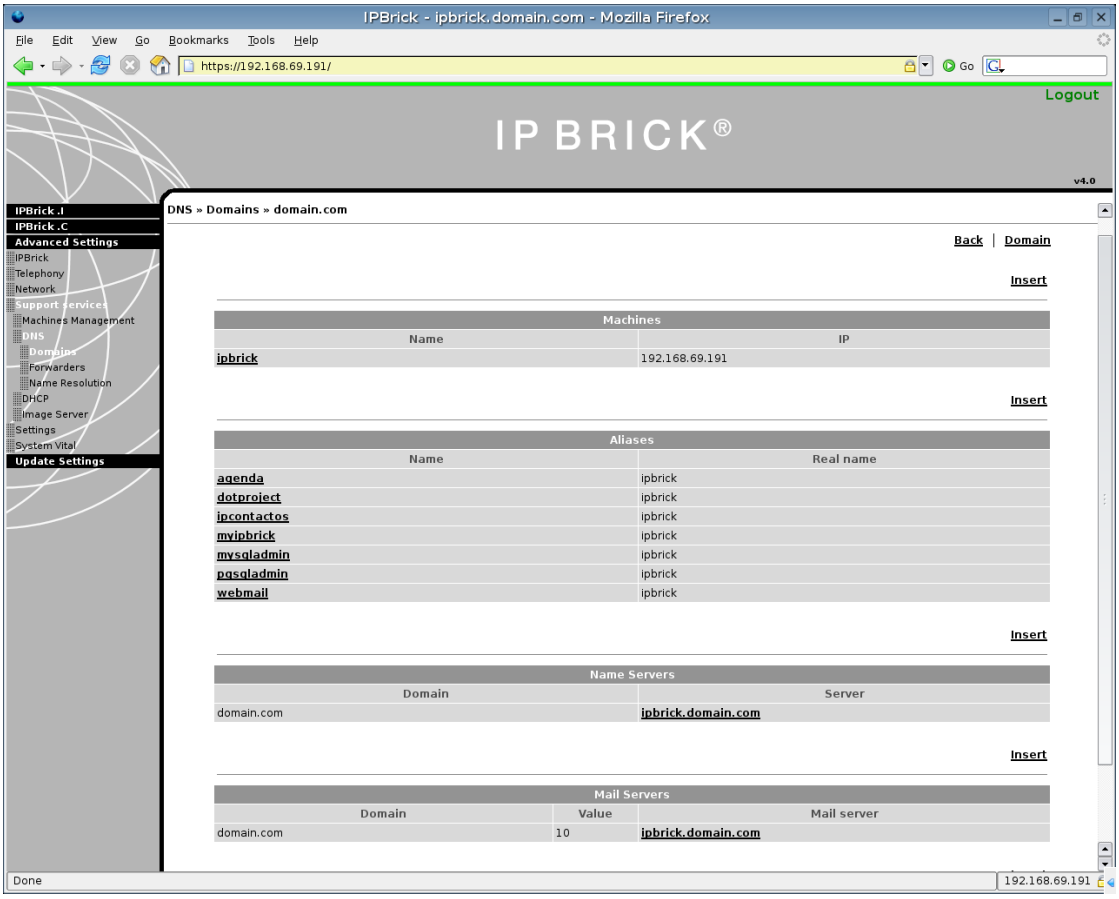

FIG. 5.15 – DNS - Gestion de domaines

2. `Aliases` : registres de *alias* pour des machines du domaine (un second nom pour une machine déjà avec nom attribué). Ette option est seulement disponible si la zone est de résolution directe exe :

   ```
   www   ->   myipbrick
   ```

3. `Serveurs de noms` : registre des adresses FQDN de machines qui servent (DNS) ce domaine, exe :

   ```
   domain.com  ->  myipbrick.domain.com
   ```

4. `Serveurs de mail` : registre des serveurs de mail pour ce domaine. Ces registres peuvent être plusieurs et distingués par des valeurs entières positives différentes, ces valeurs indiquent la préférence à être utilisée, de valeur plus basse sera toujours préféré. La valeur ici introduite devra être le FQDN du serveur de mail à introduire, soit un serveur dans le domaine lui-même, ex `empresa.pt`, soit soit un serveur dans l'Internet, exe `mail.saturno.com`. Cette option est seulement disponible si la zone est de résolution directe. Ex. :

   ```
   20 mail.saturno.com
   10 ipbrick.empresa.pt
   ```

5. `Serveurs de VoIp` : registre des serveurs de VoIP pour ce domaine. La valeur ici introduite devra être le FQDN du serveur de VoIP à introduire, exe : `voip.empresa.pt`.. Cette option est seulement disponible si la zone est de résolution directe. Exe :

   ```
   voip.empresa.pt
   ```

Forwarders

Présentation

Quand le serveur de DNS reçoit une demande pour un domaine qui n'est pas en train de servir ni l'a dans cache, doit aller chercher décider cette demande près d'autres serveurs de DNS dans l'Internet. Les forwarders devront être les plus proches, normalement les serveurs DNS de ISP. Ici vous avez l'interface propre pour enregistrer les plus proches serveurs de DNS. (Fig. 5.16)

Résolution des Noms

Présentation

Indépendamment du service DNS être en exécution ou non dans ce serveur, vous pourrez configurer ce serveur pour décider leurs demandes DNS dans un autre serveur que non le propre. Cette conFiguretion s'applique tous les services du serveur (en excluant évidemment le service DNS, qui utilisera leurs forwarders pour les demandes qui ne connaissent pas). Pour le serveur utilise sa propre DNS devra être configuré l'adresse IP de la *localhost*[8], `127.0.0.1`. (Fig. 5.17)

[7] Nom Alternatif
[8] Serveur local.

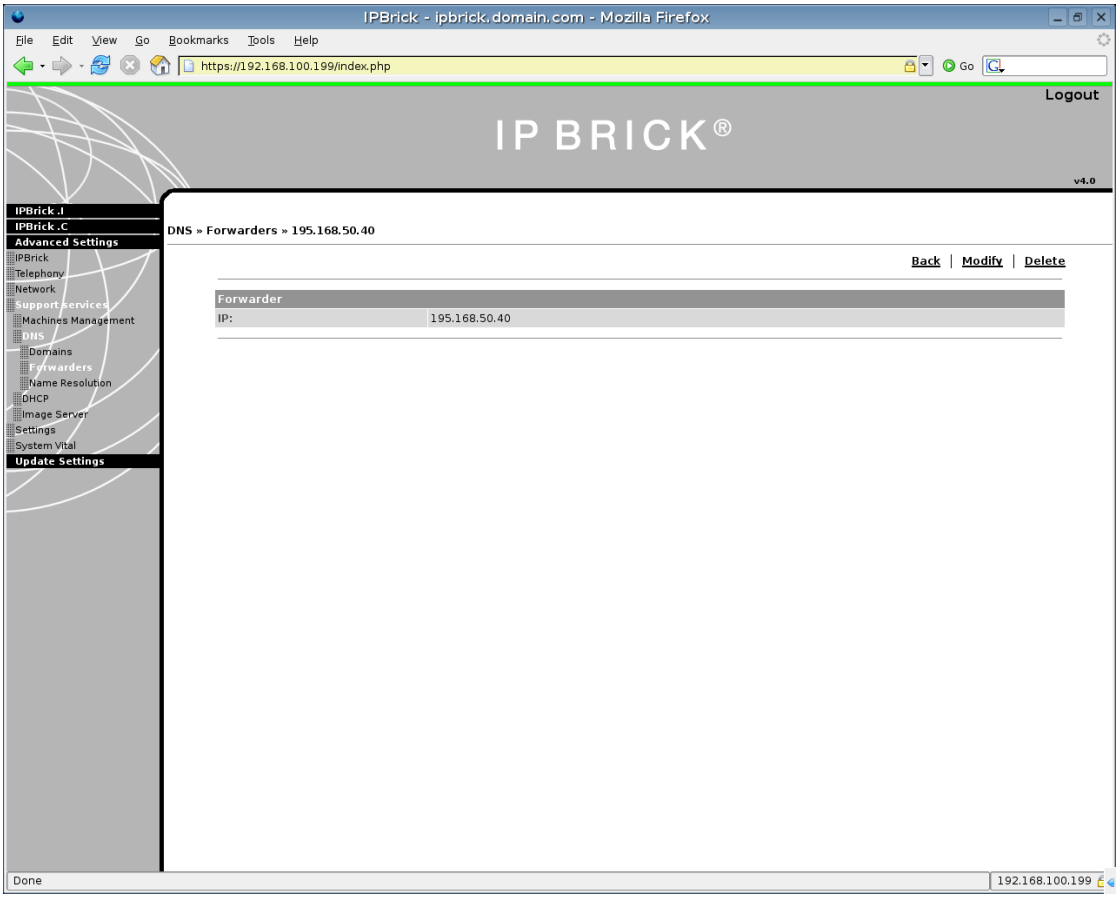

FIG. 5.16 – DNS - Forwarders

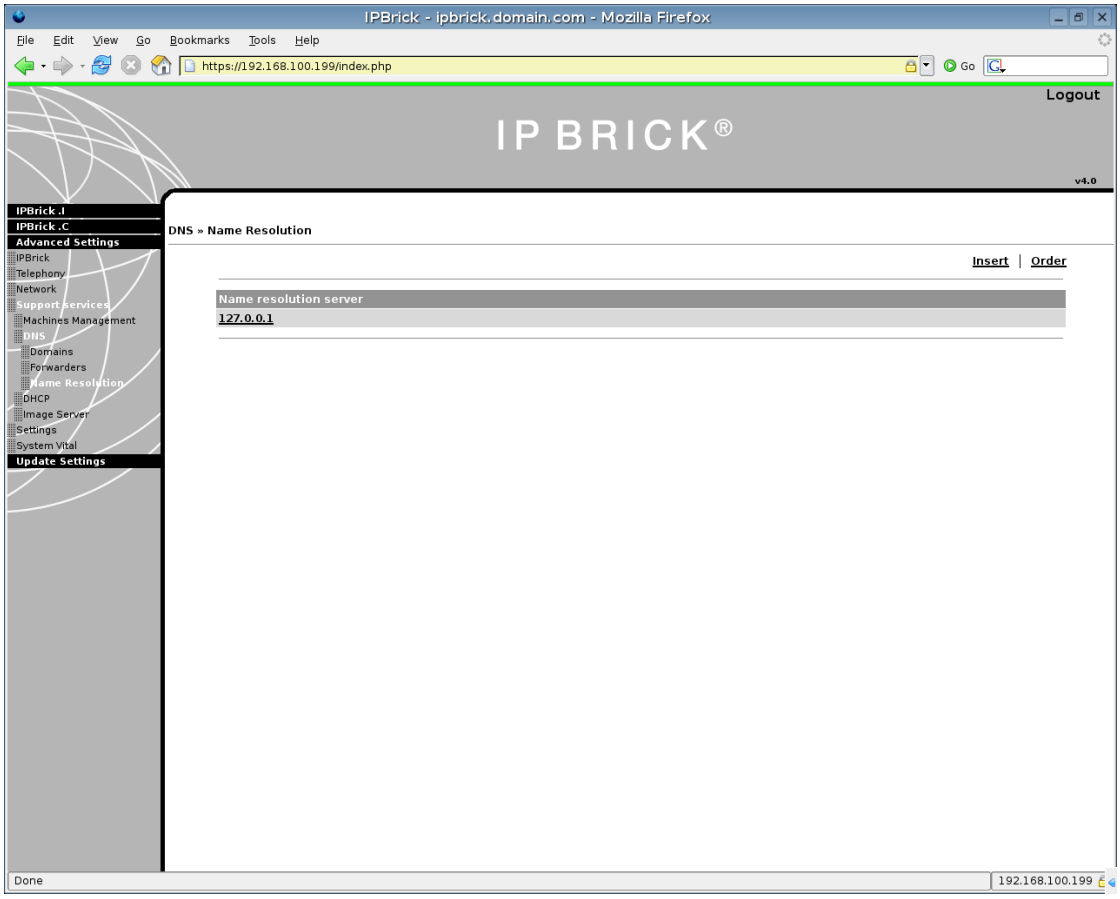

FIG. 5.17 – DNS - Résolution des Noms

5.4.3 DHCP

Sub-réseau

Présentation

Section de configuration de DHCP. Ici nous définissons sub-réseau à être servi et les paramètres des configurations de réseau à attribuer aux machines. (Fig. 5.18)

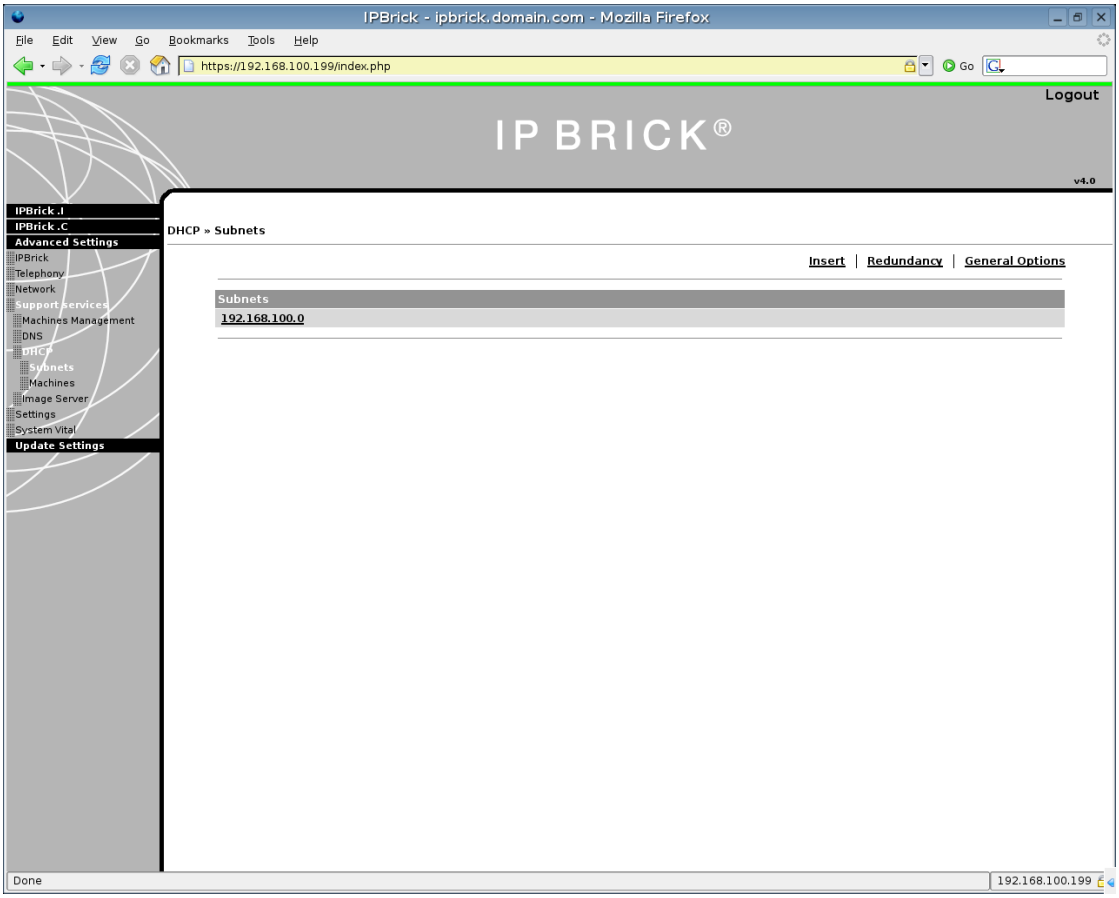

Fig. 5.18 – DHCP - Sub-réseau

Menu Dessus

Connexions pour `Insérer` nouveau sub-réseau, configurer les paramètres de `redondance` et pour définir les `Options Générales` à attribuer par défaut (voir Fig. 5.19)

Corpus

Liste de sub-réseau inséré. Chaque ligne est un lien pour formulaire de configuration des options de configuration pour respective sub filet (voir Fig. 5.20).

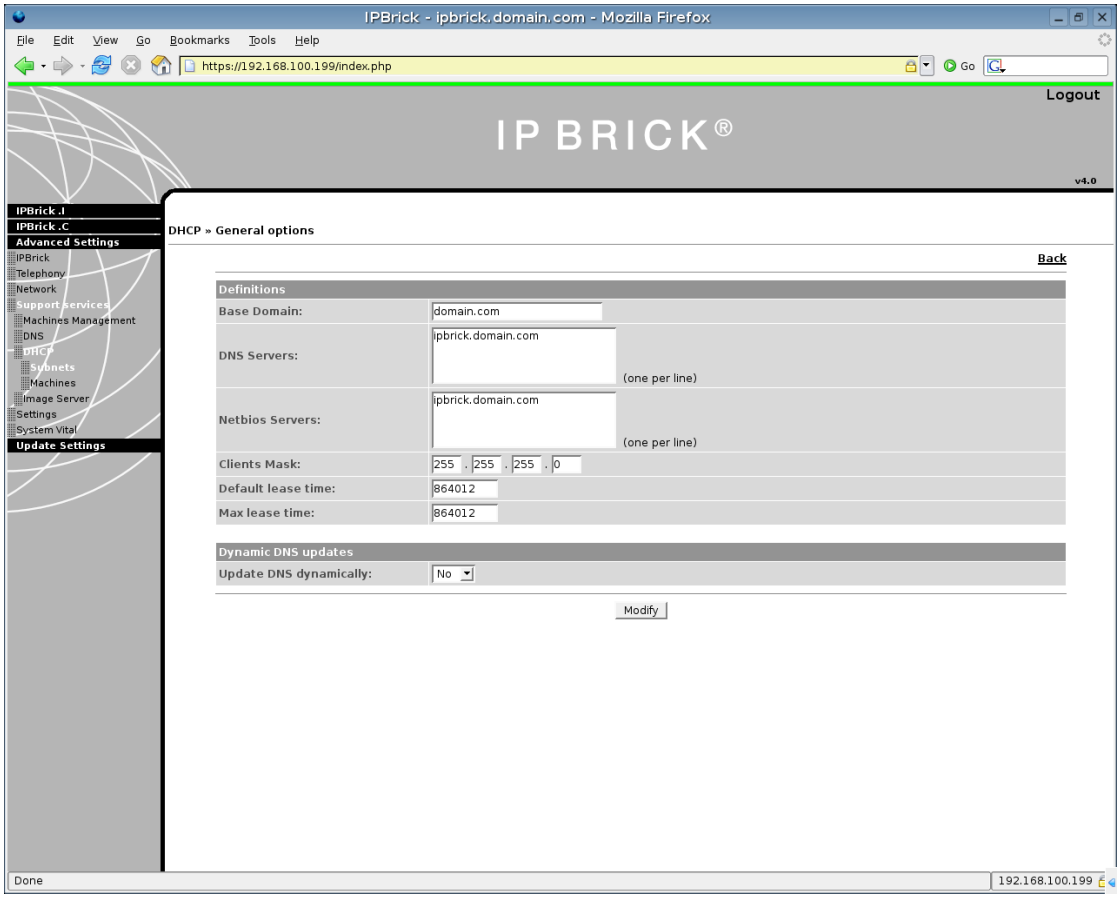

FIG. 5.19 – DHCP - Définitions Avancées

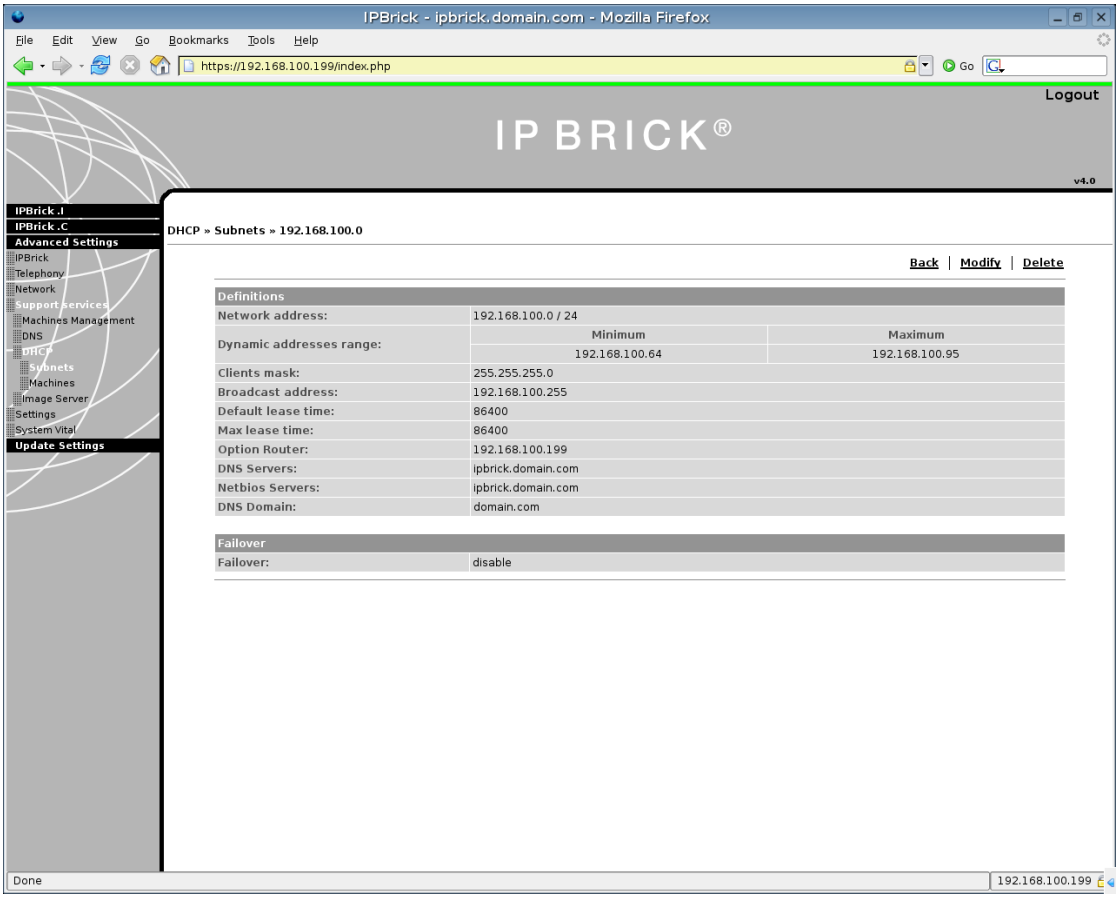

FIG. 5.20 – DHCP - Définitions Sub-réseau

Insérer

Présentation
Permet d' insérer des sous-réseaux.

Menu Principal
Liaison pour `Retourner`.

Corps
Permet d' insérer des données dans le sous-réseau, qui seront attribuées au clients. Ces données sont les suivantes :

- Adresse de Réseau : indiquer ici l' adresse du réseau et son masque ;
- Gamme d' adresses dinamiques : quelle est la gamme d' adresses réservée aux clients ;
- Masque Clients : le masque de réseau à attribuer aux clients ;
- Adresse de Broadcast : l' adresse de broadcast à attribuer aux clients ;
- Default lease time : le temps par défaut pendant lequel l' emprunt de l' adresse est valable ;
- Max lease time : le temps maximum ;
- Option Router : l' adresse du routeur qui servira comme route par défaut ;
- Serveurs DNS : une liste (un par ligne) des serveurs DNS à utiliser par les clients ;
- Serveurs NetBios : une liste (un par ligne) des serveurs NetBios à utiliser par les clients ;
- Domaine DNS : le nom du domaine indiqué aux clients.

Options Générales

Présentation
Permet d' insérer des données qui sont attribuées par défaut.

Menu Principal
Liaison pour `Retourner`.

Corps Permet d' insérer des données générales du sous-réseau, qui seront attribuées par défaut aux clients. Ces données sont les suivantes :

- Domaine base ;
- Serveurs DNS ;
- Serveurs NetBios ;
- Masque clients ;
- Default lease time ;
- Max lease time ;

On peut aussi faire l' `Actualisation Dinamique du DNS` si l' on souhaite. En ce cas, on doit choisir "OUI" sur la boîte respective.

Redondance

Présentation

Dans un réseau peut seulement exister un serveur de DHCP, à moins que se configure deux serveurs, comme primaire et secondaire respectivement. Cette fonctionnalité nous permet d'avoir de la redondance dans le service de DHCP depuis que se configure un canal de communication (connexion) entre le primaire et le secondair (voir Fig. 5.21)

Menu Dessus

Connexions pour `détourner` et pour `insérer` une nouvelle Connexion.

Corpus

Liste des Connexions insérées. Chaque ligne est un lien pour formulaire de configuration des Connexions.

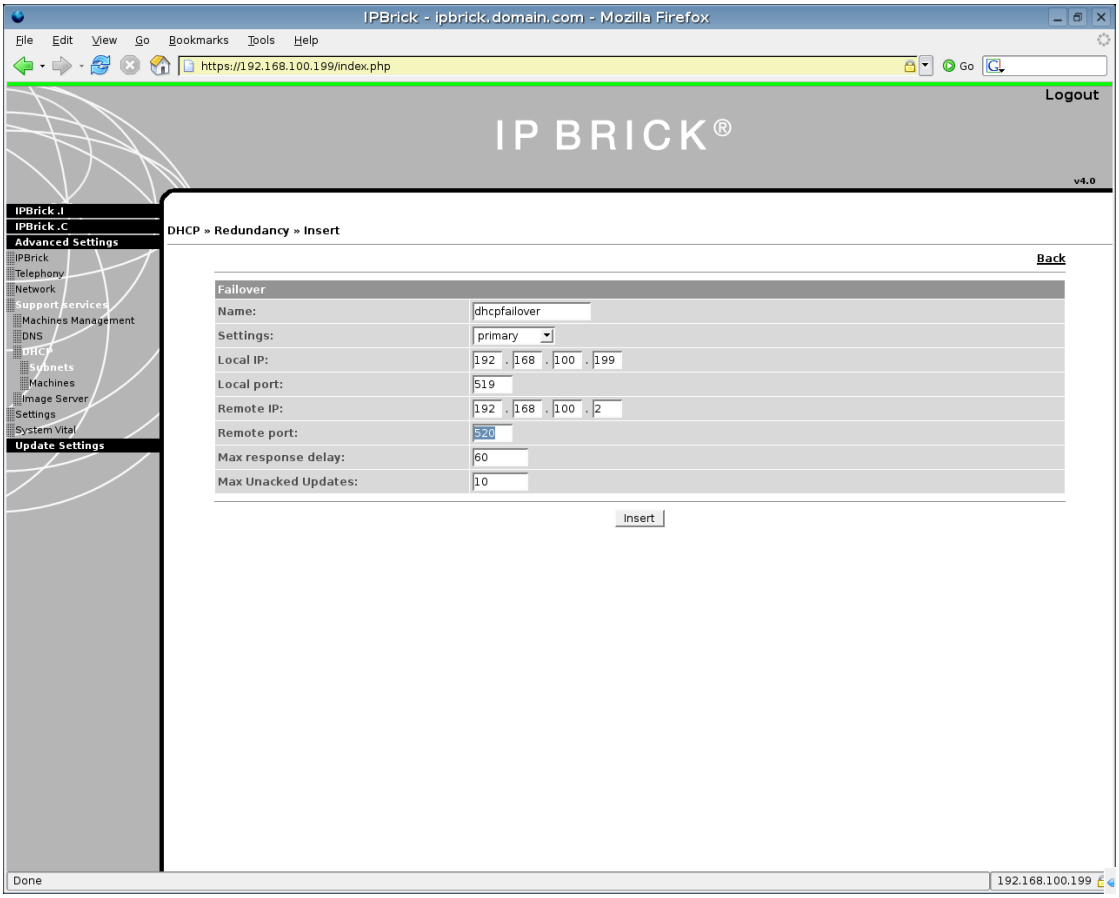

Fig. 5.21 – Redondance

Machines

Présentation

Liste des machines enregistrées avec son adresse MAC au service DHCP. Le registre de ces machines se fait à travers `Gestion de Machines` (voir section 3.1, page 15) ou directement dans cette section.

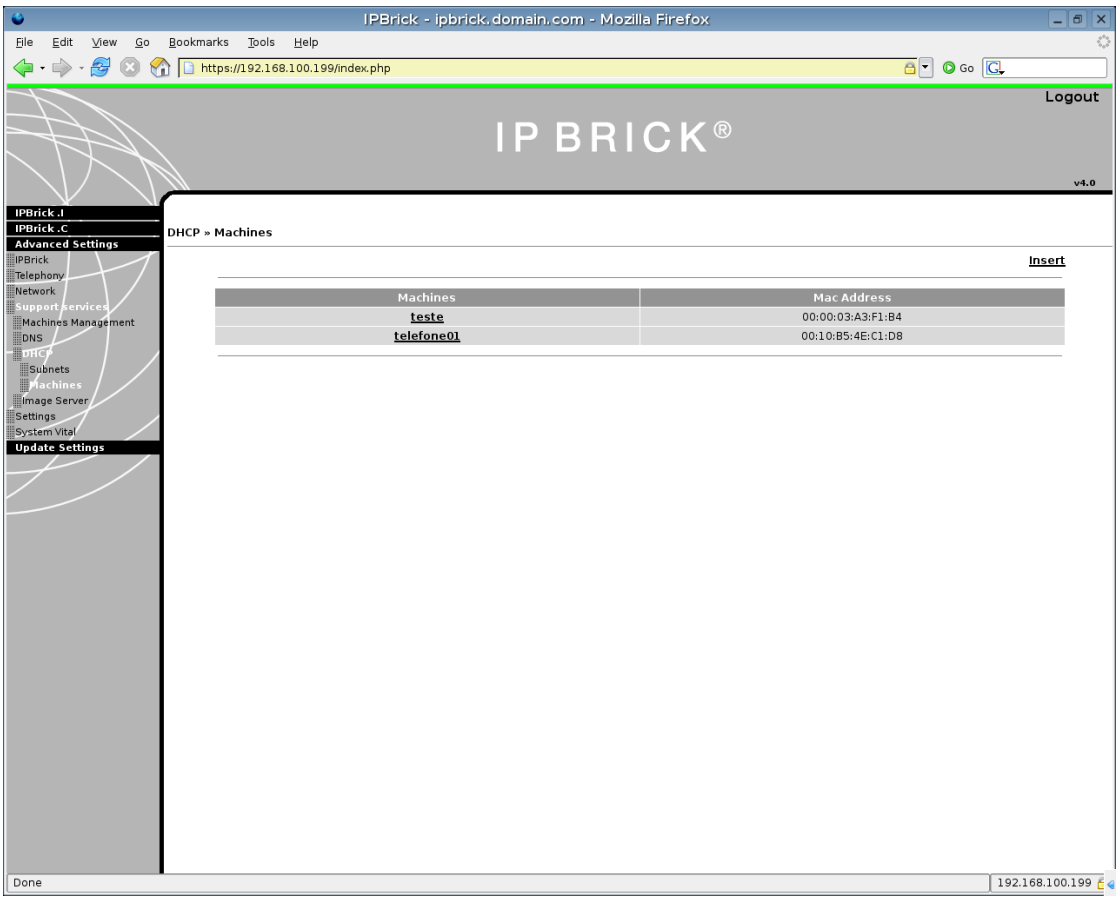

FIG. 5.22 – DHCP - Machines

5.4.4 Serveur de Machines

Cette interface se rapporte au service de réponse d'images de stations client LINUX.

Gestion d'images

Dans cette interface est effectué l'insertion d'images de stations client à partir d'un CD. Ici, il est aussi possible voir des informations sur les images présentes dans *IPBrick*, ainsi que sa dimension dans disque.

Clients

Visualisation des associations entre les machines enregistrées à l'*IPBrick* et respectives images (s'exister).

5.5 Configuration

Tous les Configuration réalisées dans *IPBrick* à travers l'interface Web ils sont gardés dans une Base de Données. De forme que, quelque modification réalisée seulement se devient accomplit le système après réaliser `Actualiser Définitions`.

En plus, au mettre à jour les Définitions de *IPBrick*, il est automatiquement gardé une copie de toutes les Configuration dans un dispositif externe, plus concrètement dans un pen USB.

! Attention: Le serveur où elle est installée *IPBrick* doit avoir toujours un pen USB allumée.

Dans celui-là, seront gardés les copies du Configuration réalisées. À partir de celui-là, il est possible récupérer les Configurations réalisées dans *IPBrick*.

Chaque copie existante à le pen USB est énumérée avec des informations de la date et de l'heure où elle a été créée.

5.5.1 Restituer

Dans cette section est présentée une liste de toutes les copies gardées dans le pen USB. Pour restituer une configuration, il est seulement nécessaire d'effectuer un clic sur la configuration prétendue (Fig. 5.23)

⇒ Remarque: À restituer une copie du configuration tous les services seront des reconfigurées. Après la configuration de tous les services, *IPBrick* ira recommencer automatiquement.

5.5.2 Télécharger

Cette section permet de décharger (*télécharger*) pour l'ordinateur local les copies des Configurations réalisées. (Fig. 5.24)

Cette option est utile pour qu'ils puissent garder dans une autre localisation la Configuration de *IPBrick*.

5.5.3 Upload

Dans cette section c'est possible charger pour le serveur un fichier de Configuration préalablement déchargé. (Fig. 5.25)

! Attention: Il n'est pas possible d'utiliser des copies des Configurations d'une version de *IPBrick* dans autre version différente de *IPBrick*. Les fichiers de configuration ne sont pas compatibles entre les différentes versions de *IPBrick*.

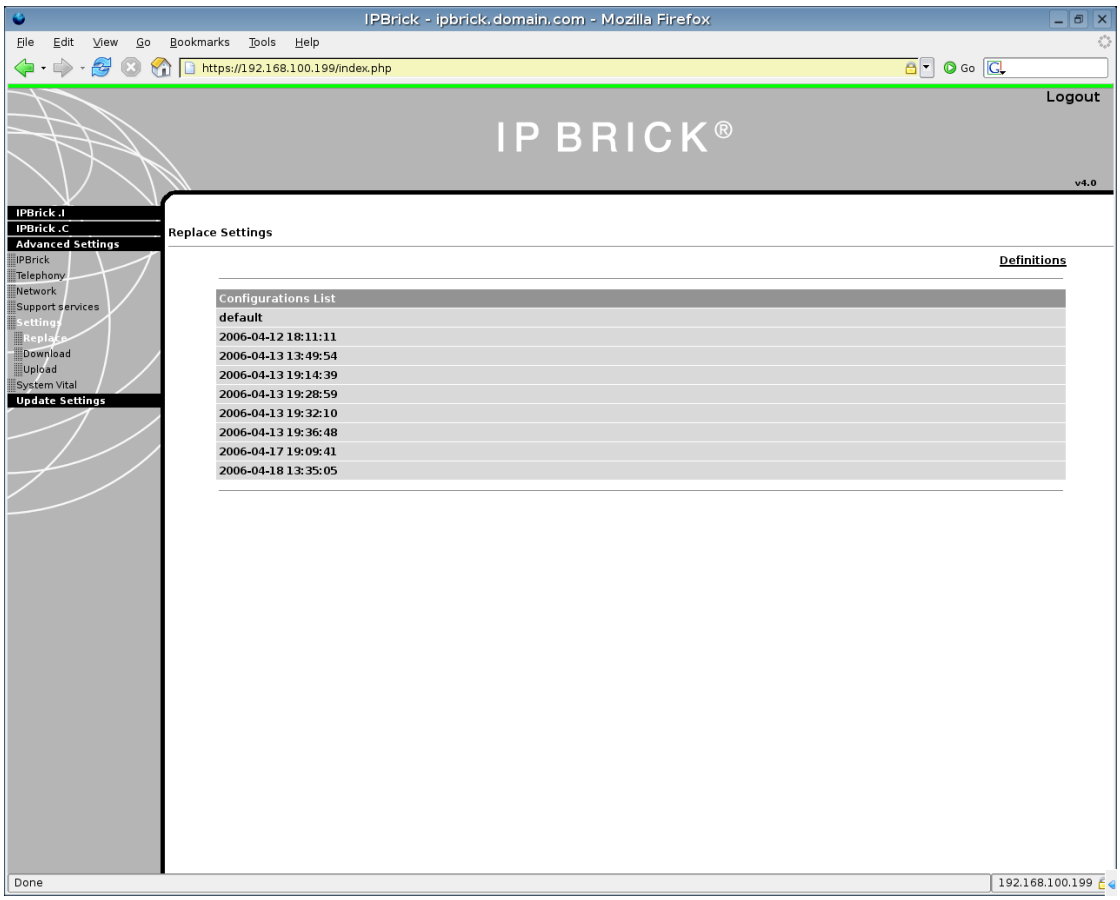

FIG. 5.23 – Restituer Configuration

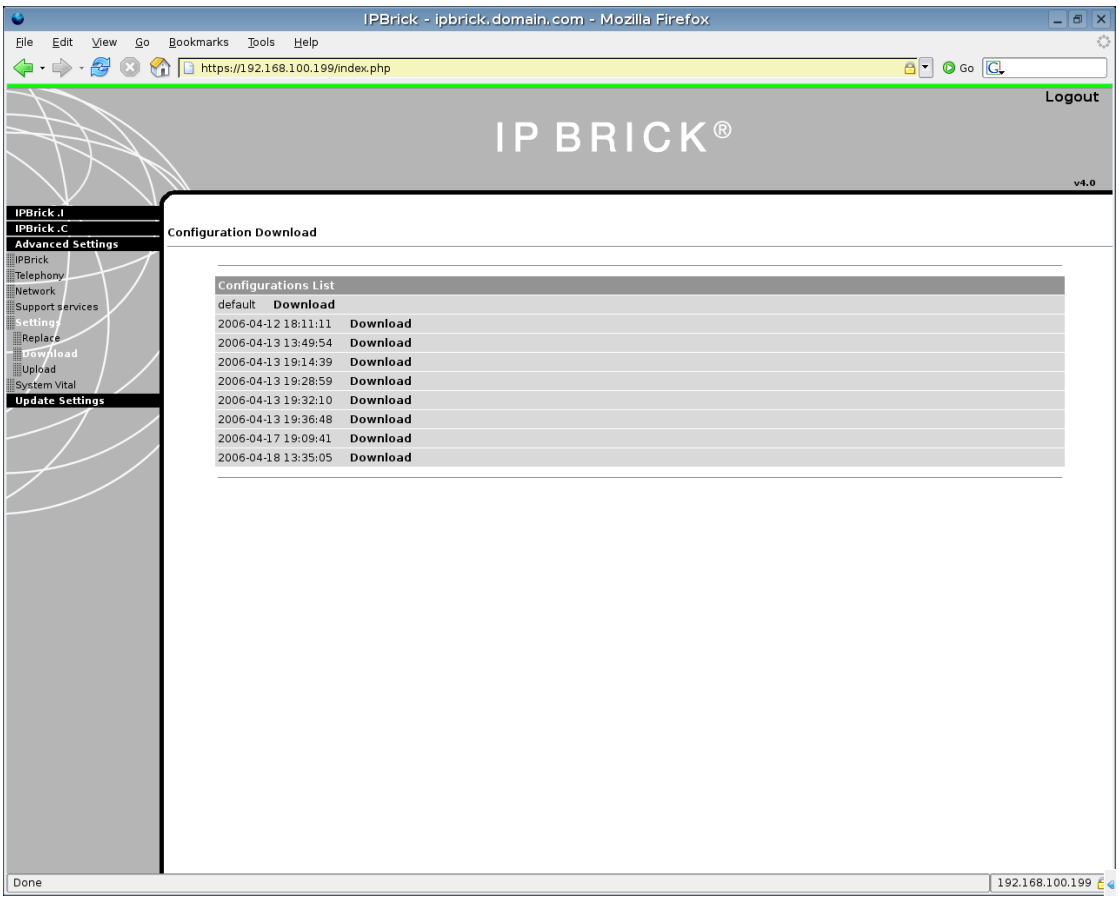

FIG. 5.24 – Décharger Configuration

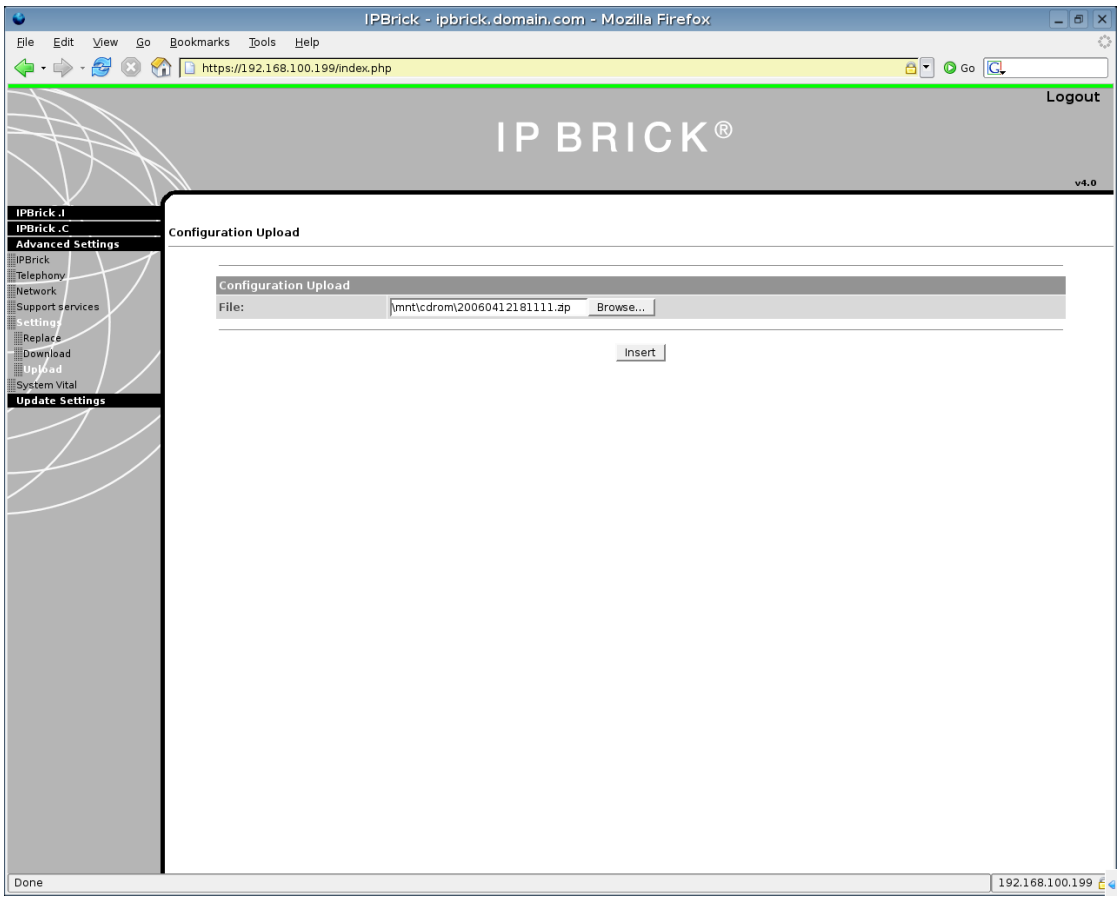

FIG. 5.25 – Charger Configuration éloignées

5.6 Système

Dans le menu Système, on peut trouver les options indiquées dans les points suivants.

5.6.1 Services

Dans les `Services` (FIG. 5.26) é est présenté une liste des plusieurs services à la disposition par *IPBrick*.

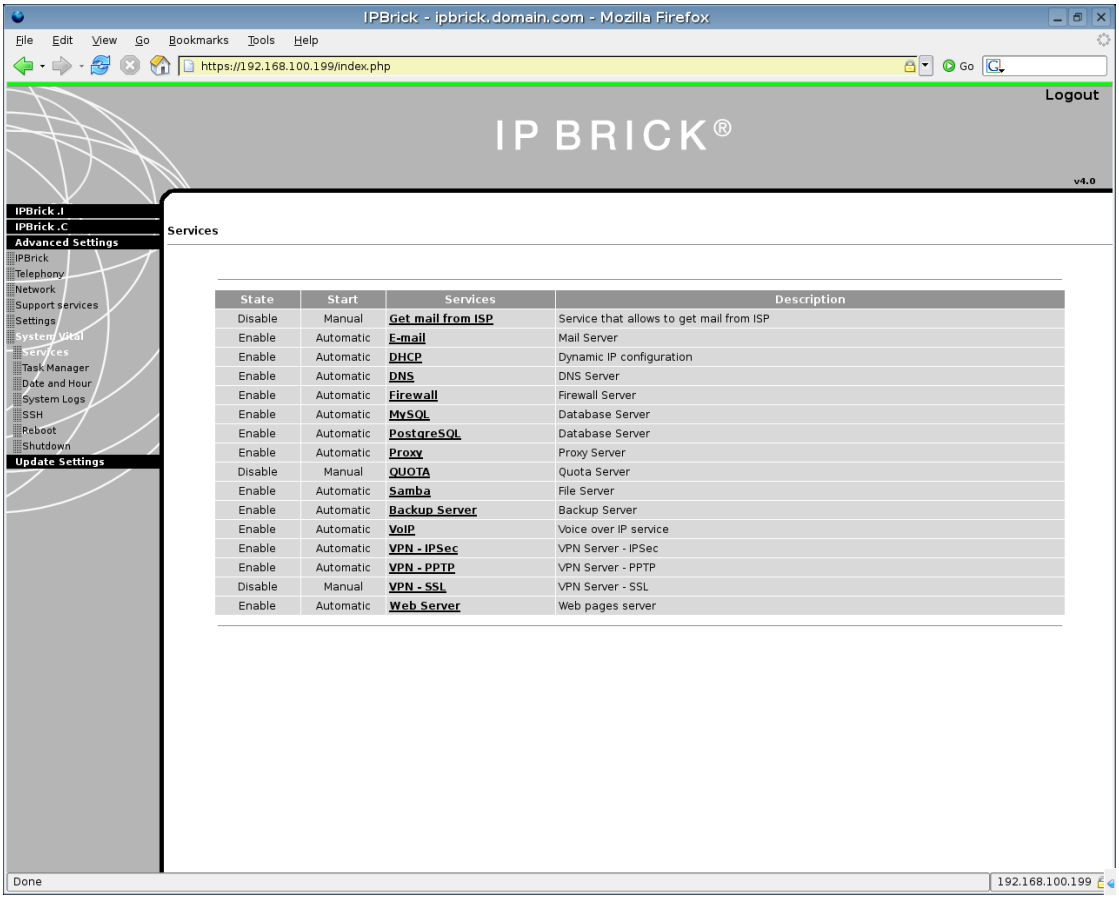

FIG. 5.26 – Services

La colonne `État` indique si le service est actif ou inactif. Ici c'est possible de recommencer quelque service sans être précis recommencer l'*IPBrick*.

Pour recommencer quelque service, vous devrez :

- Modifier son état d'Actif pour Inactif ;
- Mettre à jour les Définitions ;
- Modifier son état Inactif pour Actif ;
- Mettre à jour les Définitions.

La colonne `Arranque` définit la manière de commencement de chaque service quand le serveur est initié, soit après un reboote soit après une période où le ser-

veur a été débranché. Si pour un certain service la valeur la colonne `Arranque` fest Automatique, le service est initié automatiquement avec le commencement du serveur. D'un autre coté, si la valeur est Manuelle, ce service n'ira pas arracher automatiquement quand l'*IPBrick* soit initié. Il pourra, néanmoins, être initié manuellement dans ce menu, à travers une modification dans la valeur de la colonne `État`, qui devra être modifié Inactif pour Actif.

⇒ **Remarque: Une modification dans la valeur de la colonne `Arranque` our quelque service, il ne prend pas effet immédiat sur l'état de ce service. Cette valeur définit seulement si le service ira ou n'arracher pas automatiquement dans le proche commencement du serveur. D'autre part, une modification dans la valeur de la colonne `État` a des effets immédiats. 'est-à-dire, au modifier l'état d'un service d'Actif pour que Inactif l'*IPBrick* va arrêter ce service (après un clic sur `Actualiser Définitions`).**

5.6.2 Gestion de tâches

Le Directeur de Tâches présente une liste de tous les processus dans exécution dans l'*IPBrick*.

Cette information contient :

– Le nom de l'utilisateur du système qui a initié le processus
– La date de commencement du processus
– Le pourcentage de mémoire et de CPU que le processus est en train d'utiliser

Dans cette section c'est possible de finir un certain processus. Pour cela, c'est seulement nécessaire de faire un clic dans l'identification de ce processus.

! Attention: D'une forme générale, les processus, en exécution, ne doivent pas être finis de cette forme. Finir un processus dans cette interface pourra causer instabilité dans l'*IPBrick*. Pour définir un service, utiliser le menu `Services`.

5.6.3 Date et l'heure

Dans ce menu (Fig.5.27) c'est possible voir et modifier, la date et l'heure du serveur.

5.6.4 Logs du Système

Dans ce menu c'est possible de voir logs de l'*IPBrick*. Les Logs constituent une source d'informations importantes sur le fonctionnement du système. L'information le plus récente est disponible dans `Log Actuel`. Au cas où il y aurait autres registres de logs, ils disent respect les informations produites par l'*IPBrick* jusqu'à la date qu'ils indiquent. (Fig. 5.28).

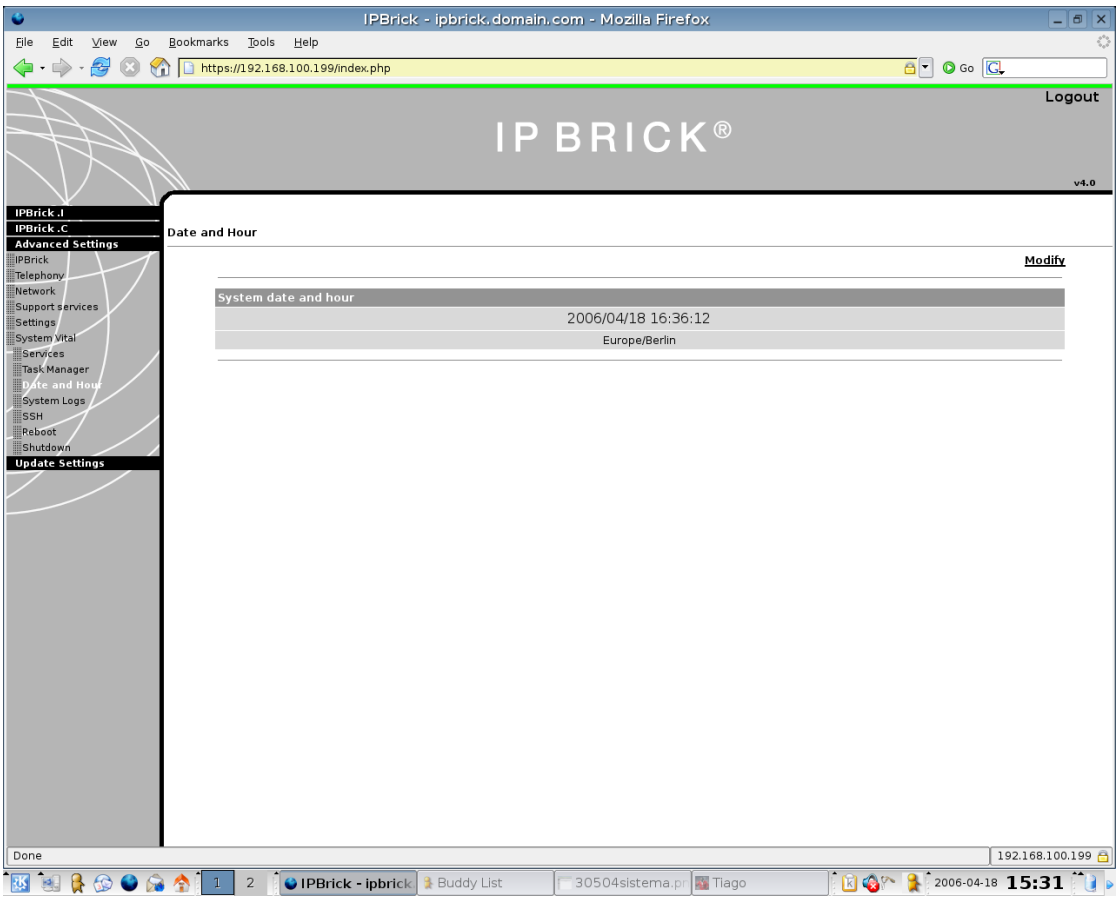

FIG. 5.27 – Date et l'heure du système

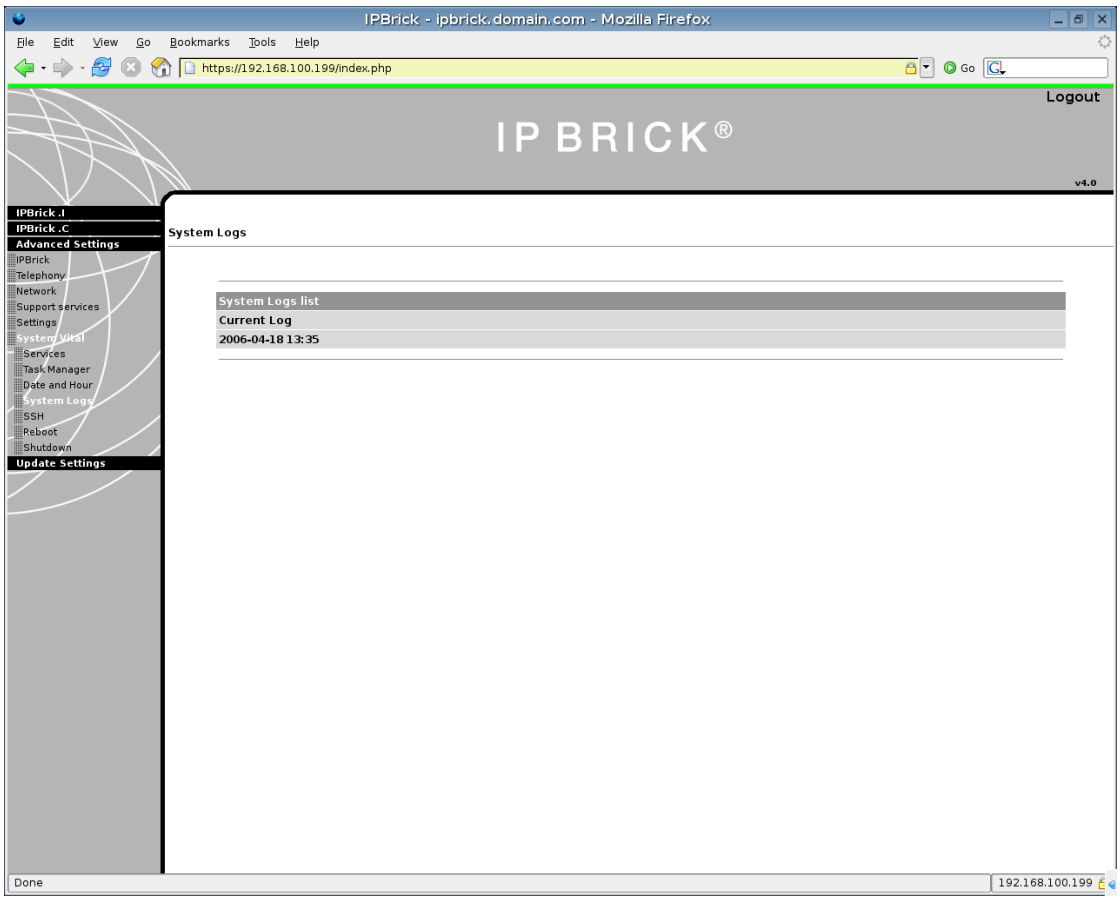

FIG. 5.28 – Logs du Système

5.6.5 SSH

Le menu SSH (FIG. 5.29) implémente une connexion secoure à *shell* l'*IPBrick*.

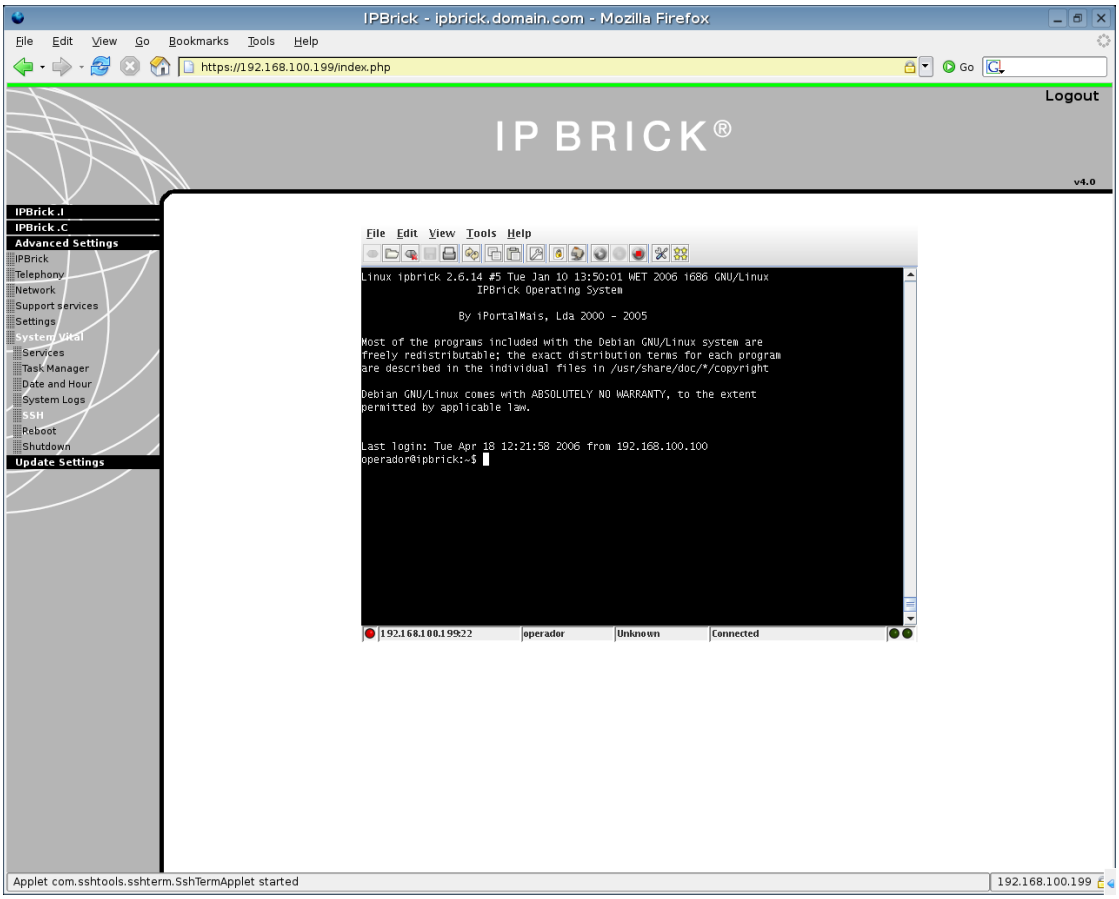

FIG. 5.29 – SSH

Le SSH (Secoure Shell) éest semblable à la connue application *Telnet*, mais plus sûre.

⇒ **Remarque: Cette fonctionnalité a besoin que le *Java Virtual Machine* soit installé. Ce logiciel est disponible dans `www.java.com`.**

Avant établir la connexion, il faut faire une authentification. Les données nécessaires sont :

- Nom de l'utilisateur : operador
- Mot de passe : L1opardo

5.6.6 Recommencer

Cette option permet recommencer l'*IPBrick* (FIG. 5.30). Après confirmer l'option de recommencer, il est automatiquement fini la connexion web au serveur.

Quand l'*IPBrick* arrachera, il est possible d'établir une nouvelle connexion https au serveur.

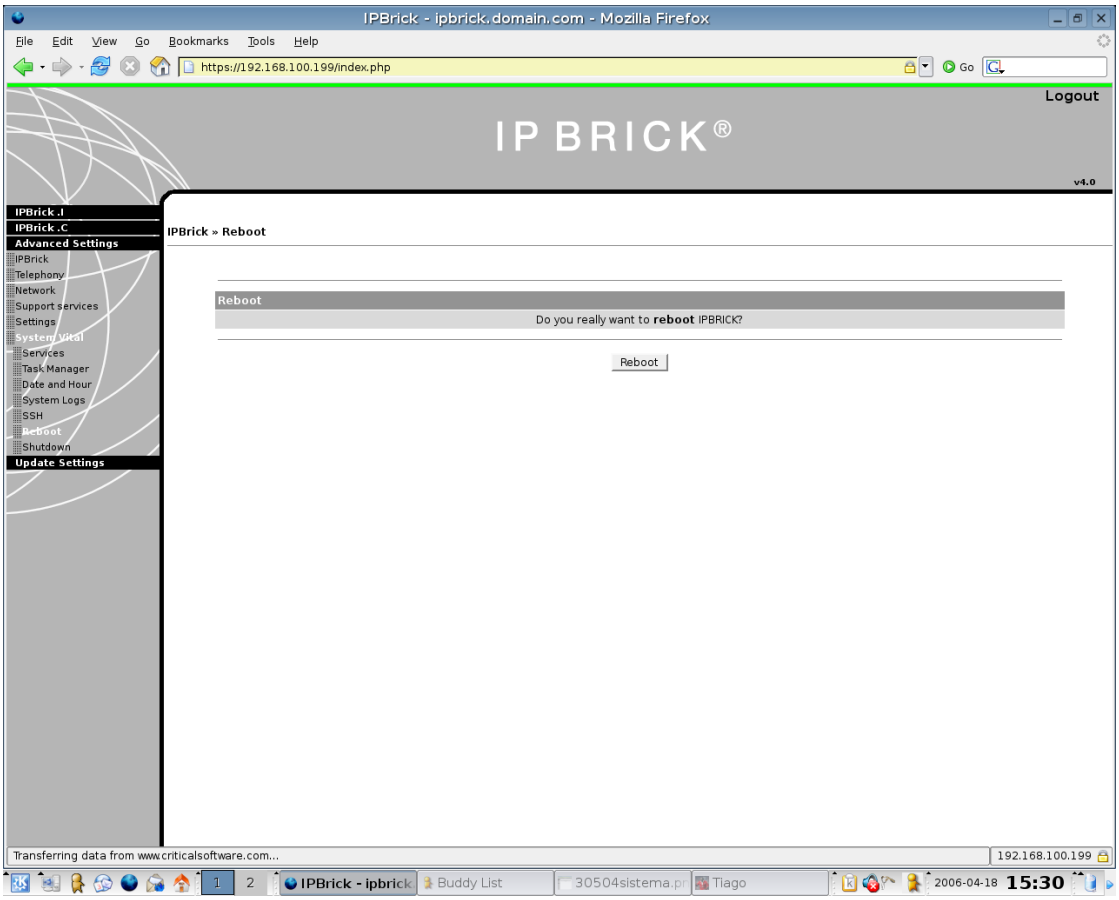

FIG. 5.30 – Recommencer le Serveur

5.6.7 Débrancher

Cette option sert à arrêter l'*IPBrick* (FIG. 5.31), en assurant que tous les services s' arrêtent correctement. A chaque fois qu' il faudra arrêter l' *IPBrick*, ce menu doit être consulté.

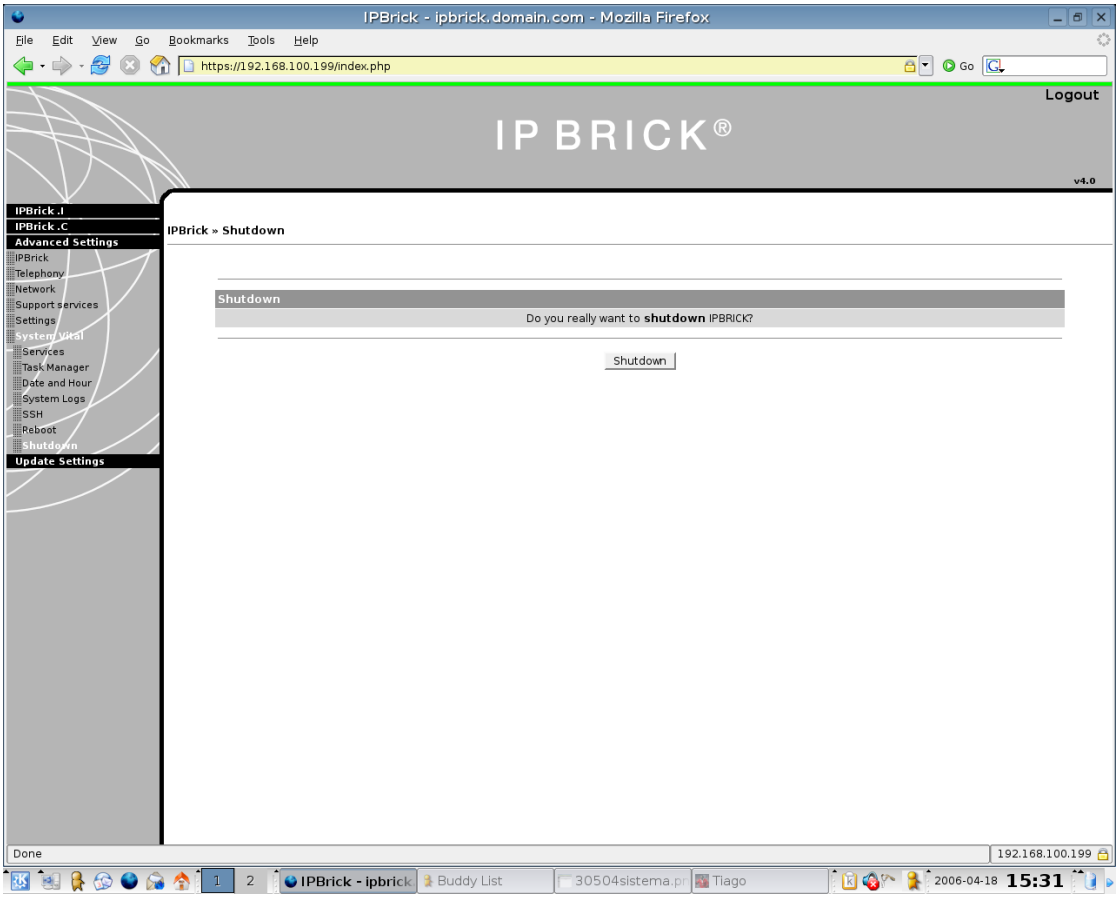

FIG. 5.31 – Débrancher le serveur

Chapitre 6

Actualiser les Définitions

L'option *Actualiser les Définitions* (Fig. 5.29) est utilisée pour que les configurations effectuées sur l'*IPBrick*deviennent effectives, c'est-à-dire, n'importe qu'elle configuration effectuée ne fonctionnera qu'après que l'administrateur de l'*IPBrick*effectue une `Actualiser les Définitions`.

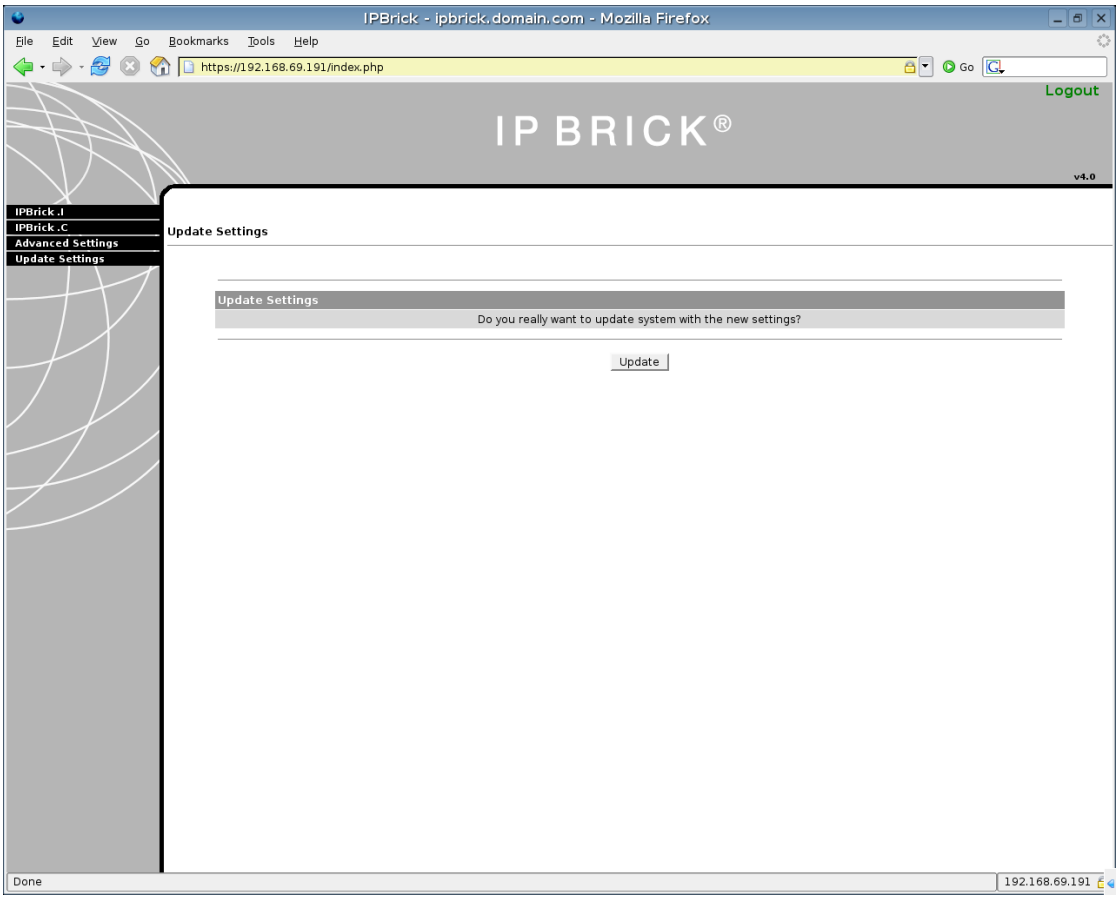

Fig. 6.1 – Actualiser les Définitions

Chapitre 7

Annexe A
Placement du domaine

7.1 Placement d'une machine dans un domaine

Placement d'une machine dans un domaine :

- Configuration d'un poste de travail avec DHCP ;
- Placement d'un poste de travail dans un domaine ;

Cette description de procédures est basée dans les suivants présupposés :

- le serveur qui contrôle le domaine est une *IPBrick.I* ;
- le domaine de DNS est l'**entreprise.fr** ;
- le domaine est la **EMPRESA**.

Pour placer un poste de travail dans un domaine c'est nécessaire d'effectuer préalablement les suivantes étapes :

1. Savoir l'adresse MAC de la plaque de réseau de la machine ;
2. Choisir une "nome"para la machine ;
3. Avoir une adresse IP pour attribuer à la machine ;
4. Créer une entrée dans l'*IPBrick.I* pour la machine ;
5. Actualiser *IPBrick.I*.

7.1.1 Postes de travaille Windows XP Professionnel

⇒ **Remarque: Avant d'initier le processus de placement d'une machine dans un domaine, il faut connaître un nom de l'utilisateur/mot de passe d'un utilisateur qui est administratif de la machine XP avant initier le processus de migration. La première étape consiste à placer la machine configurée avec DHCP.**

Pour faire ça, exécuter :

1. Faire pression dans la touche [windows] ;

2. Choisir *Mes locaux dans le réseau* ;
3. Choisir *Voir Connexions de réseau* ;
4. Cliquer le bouton droit de la souris dans l'icône *Connexion d'arie local* et choisir *Propriétés* ;
5. Dans la fenêtre qui apparaît, choisir, TCP/IP et cliquer en *Propriétés* ;
6. Dans la fenêtre qui apparaît, choisir *Obtenir l'adresse IP automatiquement* et *Obtenir l'adresse des serveurs DNS automatiquement* ;
7. Fermer les fenêtres des propriétés de réseau.

La proche étape est confirmer si l'adresse IP que la machine a obtenu, il est le même qui s'est introduite dans l'*IPBrick.I*. Pour cela, d'exécuter :

1. Faire pression les touches [windows]+[R] ;
2. cmd [ENTER] ;
3. ipconfig /all ;
4. Dans le information qui est apparue dans la fenêtre, vérifier le champ *Addresse IP*.

Au cas où l'adresse IP n'est pas le même qui s'est introduit dans l'*IPBrick*, devra être libéré et être renouvelé à travers les commandes :

1. Faire pression les touches [windows]+[R] ;
2. cmd [ENTER] ;
3. ipconfig /release ;
4. ipconfig /renew ;
5. ipconfig /all ;

Quand la machine sera déjà avec l'adresse IP prétendue, c'est possible placer la machine dans le domain **EMPRESA** :

1. Faire pression les touches [windows]+[pause] pour ouvrir les *Propriétés du Système* ;
2. Choisir *Nom de l'ordinateur*, cliquer *Changer* et nommer l'ordinateur (ce nom doit être créé préalablement dans l'*IPBrick.I*) ;
3. Cliquer sur la touche "Plus..." et additionner le domaine DNS de la machine : **entreprise.fr**. Ne laissez pas selectionné l' option *Modifier le sufixe DNS primaire lorsque vous modifiez l' association au domaine* ;
4. Dans Domaine, placera **EMPRESA**. Il sera demandé lem mot de passe d'administrator du domaine **EMPRESA** ou de l'administrateur de la machine ;
5. Cliquer OK et sortir des *Propriétés du Système*.
6. Installer le WinXPSignOnSeal (ça change une entrée dans la registre de la machine). Pour cela, copier le fichier pour la machine. Cliquer avec le bouton droit de la souris et choisir l'option Ajouter ;

7. Recommencer la machine. Quand celle-ci arrachera, vous devrez déjà être possible de faire login dans le domaine **EMPRESA**.

⇒ **Remarque: Le poste de travail n'a pas nécessairement d'être avec DHCP. Il peut être configuré avec une adresse IP fixe. S'il est le cas, quand vous enregistrez la machine dans l'*IPBrick* n'est pas nécessaire de remplir le champ Mac Address.**

Chapitre 8

Annexe B
Placement d'une connexion VPN

8.1 Placement d'une connexion VPN (PPTP)

Pour créer une connexion VPN dans un poste de travaille Windows XP Professionnel procéder comme suit :

1. Faire pression [windows] ;
2. Choisir *Panneau Contrôle* ;
3. Cliquer deux fois sur des *Connexions de Réseau*
4. Dans la fenêtre *connexions de Réseau*, choisir *Créer une nouvelle connexion* ;
5. Il apparaît le MAgicien pour la création d'une nouvelle connexion. Choisir *Connecter au réseau dans mon local de travail* (ça fait référence dans la description VPN), *Connexion de Réseau Privé Virtuel*. Ensuite choisir un nom pour que la connexion qui sera être domestique, par exemple, *Connexion à la Entreprise*. Ensuite, c'est nécessaire d'indiquer l'adresse IP ou le nom complet par lequel l'*IPBrick* est connu dans l'Internet. Finalement, choisir qui pourra utiliser la connexion VPN.

La connexion VPN est configurée. Pour établir le VPN il suffit introduire le Nom d'un utilisateur et le respective mot de passe qui soit enregistré dans l'*IPBrick* qui est en fonctionnement comme serveur VPN - PPTP.

Chapitre 9

Annexe C
Configuration d' une liaison VPN SSL (OpenVPN)

9.1 Configuration d' une liaison VPN SSL (OpenVPN)

Afin de créer une liaison VPN (OpenVPN) dans une station de travail *Windows XP Professionnel* il faut installer le software OpenVPN GUI :

- Open VPN - Packet VPN Open Source ;
- Open VPN GUI - Interface graphique pour Open VPN.

L' installation de ce paquet doit être effectuée sans modifier les définitions par défaut. Ce software este installé dans une directorie `c :\Program Files\OpenVPN`. Le certificat crée par *IPBrick* doit être décompacté dans la directorie `c :\Program Files\OpenVPN\config`.

Pour initialiser la liaison VPN, cliquer avec le bouton droit sur le icône OpenVPN sur la barre de tâches, sélectionner la liaison souhaitée et cliquer su *Connect*.

Insérer le mot-de-passe utilisé lors de la création du certificat *IPBrick* et la liaison VPN sera établie.

9.1.1 Deux ou plus certificats SSL

Quand on veut mettre plus d' un certificat dans la même station de travail (créer des liaisons VPN pour divers endroits), il faut faire le suivant avant de mettre les certificats dans la directorie `c :\Program Files\OpenVPN\config` :

1. Modifier le nom du fichier ca.crt, p.e., par ca1.crt
2. Editer le fichier ¡nom_certificat¿.ovpn et modifier la ligne avec l' entrée *ca ca.crt* par *ca ca1.crt*.

Ensuite copier les 4 fichiers qui composent le certificat dans la directorie `c :\Program Files\OpenVPN\config`.